BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2000－123084
（P2000－123084A）
(43)公開日　平成12年４月28日(2000.4.28)

(51)Int.Cl.⁷		識別記号	FI		テーマコード（参考）
G06F	17/60		G06F	15/21 Z	5B049
	13/00	351		13/00 351G	5B089
G09C	1/00	660	G09C	1/00 660B	5J104
				660E	5K025
	5/00			5/00	5K030

審査請求　未請求　請求項の数７　ＯＬ　（全 69 頁）　最終頁に続く

(21)出願番号　特願平10－293830

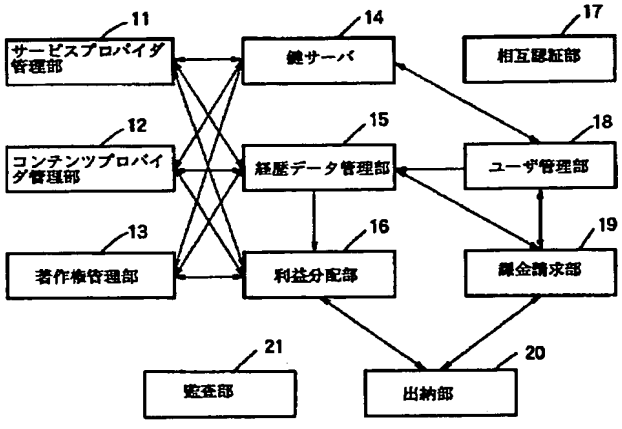
(22)出願日　平成10年10月15日(1998.10.15)

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号
(72)発明者　松山　科子
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(74)代理人　100082131
弁理士　稲本　義雄

最終頁に続く

(54)【発明の名称】　情報処理装置、情報処理方法、および提供媒体

(57)【要約】
【課題】　精算処理および利益の算出の処理を効率良く出来るようにする。
【解決手段】　利益分配部１６は、情報を特定するデータおよび情報の利用に対する情報提供業者の支払い金額を示すデータを記憶し、その記憶するデータを基に、情報提供業者毎の支払い金額の合計を算出する。出納部２０は、利益分配部１６が算出した情報提供業者毎の利益を基に、決済機関に対し情報提供業者毎の決済を指示する。



EMD サービスセンタ 1

1

【特許請求の範囲】

【請求項１】　情報提供業者に代わり、前記情報提供業者が提供する情報の利用者から利用料金を徴収し、情報提供業者に利益を分配する情報処理装置において、

前記情報を特定するデータおよび前記情報の利用に対する前記情報提供業者への支払い金額を示すデータを記憶する記憶手段と、

前記記憶手段が記憶するデータを基に、前記情報提供業者毎への支払い金額の合計を算出する算出手段と、

前記情報提供業者毎の利益を基に、決済機関に対し前記情報提供業者毎の決済を指示する決済指示手段とを備えることを特徴とする情報処理装置。

【請求項２】前記算出手段は、前記情報提供業者間の支払金額の合計をさらに算出することを特徴とする請求項１に記載の情報処理装置。

【請求項３】　前記記憶手段は、前記情報の著作権を徴収する団体への支払い金額に関する情報をさらに記憶し、

前記算出手段は、前記団体への支払い金額の合計をさらに算出し、

前記決済指示手段は、前記決済機関に対し前記団体の決済をさらに指示することを特徴とする請求項１に記載の情報処理装置。

【請求項４】　前記記憶手段は、情報の利用料金の割引のデータをさらに記憶することを特徴とする請求項１に記載の情報処理装置。

【請求項５】　前記決済指示手段は、前記情報提供業者毎の決済機関に関する情報を記憶することを特徴とする請求項１に記載の情報処理装置。

【請求項６】　情報提供業者に代わり、前記情報提供業者が提供する情報の利用者から利用料金を徴収し、情報提供業者に利益を分配する情報処理方法において、

前記情報を特定するデータおよび前記情報の利用に対する前記情報提供業者への支払い金額を示すデータを記憶する記憶ステップと、

前記記憶ステップで記憶するデータを基に、前記情報提供業者毎への支払い金額の合計を算出する算出ステップと、

前記情報提供業者毎の利益を基に、決済機関に対し前記情報提供業者毎の決済を指示する決済指示ステップとを含むことを特徴とする情報処理方法。

【請求項７】　情報提供業者に代わり、前記情報提供業者が提供する情報の利用者から利用料金を徴収し、情報提供業者に利益を分配する情報処理装置に、

前記情報を特定するデータおよび前記情報の利用に対する前記情報提供業者への支払い金額を示すデータを記憶する記憶ステップと、

前記記憶ステップで記憶するデータを基に、前記情報提供業者毎への支払い金額の合計を算出する算出ステップと、

2

前記情報提供業者毎の利益を基に、決済機関に対し前記情報提供業者毎の決済を指示する決済指示ステップとを含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする提供媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、情報処理装置、情報処理方法、および提供媒体に関し、特に、情報提供業者に代わり、情報の利用者から利用料金を徴収し、情報提供業者に利益を分配する情報処理装置、情報処理方法、および提供媒体に関する。

【０００２】

【従来の技術】音楽などの情報を暗号化し、所定の契約を交わしたユーザの情報処理装置に送信し、ユーザは、その情報処理装置で情報を復号して、再生するシステムがある。情報提供者は、複数の情報提供者に、情報を送信し、サービスを提供することができる。

【０００３】

【発明が解決しようとする課題】情報提供者は、複数のユーザ毎に、契約し、利用料金を精算しなければならず、また、精算処理および利益の算出処理を行わなければならず、無駄が多い。

【０００４】本発明はこのような状況に鑑みてなされたものであり、精算処理および利益の算出の処理を効率良く出来るようにすることを目的とする。

【０００５】

【課題を解決するための手段】請求項１に記載の情報処理装置は、情報を特定するデータおよび情報の利用に対する情報提供業者への支払い金額を示すデータを記憶する記憶手段と、記憶手段が記憶するデータを基に、情報提供業者毎への支払い金額の合計を算出する算出手段と、情報提供業者毎の利益を基に、決済機関に対し情報提供業者毎の決済を指示する決済指示手段とを備えることを特徴とする。

【０００６】請求項６に記載の情報処理方法は、情報を特定するデータおよび情報の利用に対する情報提供業者への支払い金額を示すデータを記憶する記憶ステップと、記憶ステップで記憶するデータを基に、情報提供業者毎への支払い金額の合計を算出する算出ステップと、情報提供業者毎の利益を基に、決済機関に対し情報提供業者毎の決済を指示する決済指示ステップとを含むことを特徴とする。

【０００７】請求項７に記載の提供媒体は、情報処理装置に、情報を特定するデータおよび情報の利用に対する情報提供業者への支払い金額を示すデータを記憶する記憶ステップと、記憶ステップで記憶するデータを基に、情報提供業者毎への支払い金額の合計を算出する算出ステップと、情報提供業者毎の利益を基に、決済機関に対し情報提供業者毎の決済を指示する決済指示ステップとを含む処理を実行させるコンピュータが読み取り可能な

プログラムを提供することを特徴とする。

【０００８】請求項１に記載の情報処理装置、請求項６に記載の情報処理方法、および請求項７に記載の提供媒体においては、情報を特定するデータおよび情報の利用に対する情報提供業者への支払い金額を示すデータを記憶し、記憶するデータを基に、情報提供業者毎への支払い金額の合計を算出し、情報提供業者毎の利益を基に、決済機関に対し情報提供業者毎の決済を指示する。

【０００９】

【発明の実施の形態】以下に本発明の実施の形態を説明するが、特許請求の範囲に記載の発明の各手段と以下の実施の形態との対応関係を明らかにするために、各手段の後の括弧内に、対応する実施の形態（但し一例）を付加して本発明の特徴を記述すると、次のようになる。但し勿論この記載は、各手段を記載したものに限定することを意味するものではない。

【００１０】すなわち、請求項１に記載の情報処理装置は、情報を特定するデータおよび情報の利用に対する情報提供業者への支払い金額を示すデータを記憶する記憶手段（例えば、図２の利益分配部１６）と、記憶手段が記憶するデータを基に、情報提供業者毎への支払い金額の合計を算出する算出手段（例えば、図２の利益分配部１６）と、情報提供業者毎の利益を基に、決済機関に対し情報提供業者毎の決済を指示する決済指示手段（例えば、図２の出納部２０）とを備えることを特徴とする。

【００１１】図１は、本発明を適用したEMD(Electronic Music Distribution:電子音楽配信)システムを説明する図である。このシステムでユーザに配信されるコンテンツ(Content)とは、情報そのものが価値を有するデジタルデータをいい、以下、音楽データを例に説明する。EMDサービスセンタ１は、コンテンツプロバイダ２、ユーザホームネットワーク５等に配送用鍵Ｋｄを送信し、ユーザホームネットワーク５から、コンテンツの利用に応じた課金情報等を受信し、利用料金を精算し、コンテンツプロバイダ２およびサービスプロバイダ３への利益分配の処理を行う。

【００１２】コンテンツプロバイダ２は、デジタル化されたコンテンツを有し、自己のコンテンツであることを証明するためのウォータマーク（電子透かし）をコンテンツに挿入し、コンテンツを圧縮し、および暗号化し、所定の情報を付加して、サービスプロバイダ３に送信する。

【００１３】サービスプロバイダ３は、専用のケーブルネットワーク、インターネット、または衛星などから構成されるネットワーク４を介して、コンテンツプロバイダ２から供給されたコンテンツに価格を付して、ユーザホームネットワーク５に送信する。

【００１４】ユーザホームネットワーク５は、サービスプロバイダ３から価格を付して送付されたコンテンツを入手し、コンテンツを復号、再生して利用するとともに課金処理を実行する。課金処理により得られた課金情報は、ユーザホームネットワーク５が配送用鍵ＫｄをEMDサービスセンタ１から入手する際、EMDサービスセンタ１に送信される。

【００１５】図２は、EMDサービスセンタ１の機能の構成を示すブロック図である。サービスプロバイダ管理部１１は、サービスプロバイダ３に利益分配の情報を供給するとともに、コンテンツプロバイダ２から供給されるコンテンツに付される情報（取扱方針）が暗号化されている場合、サービスプロバイダ３に配送用鍵Ｋｄを送信する。コンテンツプロバイダ管理部１２は、コンテンツプロバイダ２に配送用鍵Ｋｄを送信するとともに、利益分配の情報を供給する。著作権管理部１３は、ユーザホームネットワーク５のコンテンツの利用の実績を示す情報を、著作権を管理する団体、例えば、JASRAC(Japanese Society for Rights of Authors,Composers and Publishers:日本音楽著作権協会)に送信する。鍵サーバ１４は、配送用鍵Ｋｄを記憶しており、コンテンツプロバイダ管理部１２、またはユーザ管理部１８等を介して、配送用鍵Ｋｄをコンテンツプロバイダ２、またはユーザホームネットワーク５等に供給する。ユーザ管理部１８は、ユーザホームネットワーク５のコンテンツの利用の実績を示す情報である課金情報、そのコンテンツに対応する価格情報、およびそのコンテンツに対応する取扱方針を入力し、経歴データ管理部１５に記憶させる。

【００１６】EMDサービスセンタ１からコンテンツプロバイダ２およびユーザホームネットワーク５を構成するレシーバ５１（図１０で後述する）への、配送用鍵Ｋｄの定期的な送信の例について、図３乃至図６を参照に説明する。図３は、コンテンツプロバイダ２がコンテンツの提供を開始し、ユーザホームネットワーク５を構成するレシーバ５１がコンテンツの利用を開始する、１９９８年１月における、EMDサービスセンタ１が有する配送用鍵Ｋｄ、コンテンツプロバイダ２が有する配送用鍵Ｋｄ、およびレシーバ５１が有する配送用鍵Ｋｄを示す図である。

【００１７】図３の例において、配送用鍵Ｋｄは、暦の月の初日から月の末日まで、使用可能であり、たとえば、所定のビット数の乱数である”ａａａａａａａａ”の値を有するバージョン１である配送用鍵Ｋｄは、１９９８年１月１日から１９９８年１月３１日まで使用可能（すなわち、１９９８年１月１日から１９９８年１月３１日の期間にサービスプロバイダ３がユーザホームネットワーク５に配布するコンテンツを暗号化するコンテンツ鍵Ｋｃｏは、バージョン１である配送用鍵Ｋｄで暗号化されている）であり、所定のビット数の乱数である”ｂｂｂｂｂｂｂｂ”の値を有するバージョン２である配送用鍵Ｋｄは、１９９８年２月１日から１９９８年２月２８日まで使用可能（すなわち、その期間にサービスプロバイダ３がユーザホームネットワーク５に配布するコ

5

ンテンツを暗号化するコンテンツ鍵Ｋｃｏは、バージョン２である配送用鍵Ｋｄで暗号化されている）である。同様に、バージョン３である配送用鍵Ｋｄは、１９９８年３月中に使用可能であり、バージョン４である配送用鍵Ｋｄは、１９９８年４月中に使用可能であり、バージョン５である配送用鍵Ｋｄは、１９９８年５月中に使用可能であり、バージョン６である配送用鍵Ｋｄは、１９９８年６月中に使用可能である。

【００１８】コンテンツプロバイダ２がコンテンツの提供を開始するに先立ち、EMDサービスセンタ１は、コンテンツプロバイダ２に、１９９８年１月から１９９８年６月まで利用可能な、バージョン１乃至バージョン６の６つの配送用鍵Ｋｄを送信し、コンテンツプロバイダ２は、６つの配送用鍵Ｋｄを受信し、記憶する。６月分の配送用鍵Ｋｄを記憶するのは、コンテンツプロバイダ２は、コンテンツを提供する前のコンテンツおよびコンテンツ鍵の暗号化などの準備に、所定の期間が必要だからである。

【００１９】また、レシーバ５１がコンテンツの利用を開始するに先立ち、EMDサービスセンタ１は、レシーバ５１に、１９９８年１月から１９９８年３月まで、利用可能なバージョン１乃至バージョン３である３つの配送用鍵Ｋｄを送信し、レシーバ５１は、３つの配送用鍵Ｋｄを受信し、記憶する。３月分の配送用鍵Ｋｄを記憶するのは、レシーバ５１が、EMDサービスセンタ１に接続できないなどのトラブルにより、コンテンツの利用が可能な契約期間にもかかわらずコンテンツが利用できない等の事態を避けるためであり、また、EMDサービスセンタ１への接続の頻度を低くし、ユーザホームネットワーク５の負荷を低減するためである。

【００２０】１９９８年１月１日から１９９８年１月３１日の期間には、バージョン１である配送用鍵Ｋｄが、EMDサービスセンタ１、コンテンツプロバイダ２、ユーザホームネットワーク５を構成するレシーバ５１で利用される。

【００２１】１９９８年２月１日における、EMDサービスセンタ１の配送用鍵Ｋｄのコンテンツプロバイダ２、およびレシーバ５１への送信を図４で説明する。EMDサービスセンタ１は、コンテンツプロバイダ２に、１９９８年２月から１９９８年７月まで利用可能な、バージョン２乃至バージョン７の６つの配送用鍵Ｋｄを送信し、コンテンツプロバイダ２は、６つの配送用鍵Ｋｄを受信し、受信前に記憶していた配送用鍵Ｋｄに上書きし、新たな配送用鍵Ｋｄを記憶する。EMDサービスセンタ１は、レシーバ５１に、１９９８年２月から１９９８年４月まで、利用可能なバージョン２乃至バージョン４である３つの配送用鍵Ｋｄを送信し、レシーバ５１は、３つの配送用鍵Ｋｄを受信し、受信前に記憶していた配送用鍵Ｋｄに上書きし、新たな配送用鍵Ｋｄを記憶する。EMDサービスセンタ１は、バージョン１である配送用鍵Ｋ

6

ｄをそのまま記憶する。これは、不測のトラブルが発生したとき、若しくは不正が発生し、または発見されたときに、過去に利用した配送用鍵Ｋｄを利用できるようにするためである。

【００２２】１９９８年２月１日から１９９８年２月２８日の期間には、バージョン２である配送用鍵Ｋｄが、EMDサービスセンタ１、コンテンツプロバイダ２、ユーザホームネットワーク５を構成するレシーバ５１で利用される。

【００２３】１９９８年３月１日における、EMDサービスセンタ１の配送用鍵Ｋｄのコンテンツプロバイダ２、およびレシーバ５１への送信を図５で説明する。EMDサービスセンタ１は、コンテンツプロバイダ２に、１９９８年３月から１９９８年８月まで利用可能な、バージョン３乃至バージョン８の６つの配送用鍵Ｋｄを送信し、コンテンツプロバイダ２は、６つの配送用鍵Ｋｄを受信し、受信前に記憶していた配送用鍵Ｋｄに上書きし、新たな配送用鍵Ｋｄを記憶する。EMDサービスセンタ１は、レシーバ５１に、１９９８年３月から１９９８年５月まで、利用可能なバージョン３乃至バージョン５である３つの配送用鍵Ｋｄを送信し、レシーバ５１は、３つの配送用鍵Ｋｄを受信し、受信前に記憶していた配送用鍵Ｋｄに上書きし、新たな配送用鍵Ｋｄを記憶する。EMDサービスセンタ１は、バージョン１である配送用鍵Ｋｄおよびバージョン２である配送用鍵Ｋｄをそのまま記憶する。

【００２４】１９９８年３月１日から１９９８年３月３１日の期間には、バージョン３である配送用鍵Ｋｄが、EMDサービスセンタ１、コンテンツプロバイダ２、ユーザホームネットワーク５を構成するレシーバ５１で利用される。

【００２５】１９９８年４月１日における、EMDサービスセンタ１の配送用鍵Ｋｄのコンテンツプロバイダ２、およびレシーバ５１への送信を図６で説明する。EMDサービスセンタ１は、コンテンツプロバイダ２に、１９９８年４月から１９９８年９月まで利用可能な、バージョン４乃至バージョン９の６つの配送用鍵Ｋｄを送信し、コンテンツプロバイダ２は、６つの配送用鍵Ｋｄを受信し、受信前に記憶していた配送用鍵Ｋｄに上書きし、新たな配送用鍵Ｋｄを記憶する。EMDサービスセンタ１は、レシーバ５１に、１９９８年４月から１９９８年６月まで、利用可能なバージョン４乃至バージョン６である３つの配送用鍵Ｋｄを送信し、レシーバ５１は、３つの配送用鍵Ｋｄを受信し、受信前に記憶していた配送用鍵Ｋｄに上書きし、新たな配送用鍵Ｋｄを記憶する。EMDサービスセンタ１は、バージョン１である配送用鍵Ｋｄ、バージョン２である配送用鍵Ｋｄ、およびバージョン３である配送用鍵Ｋｄをそのまま記憶する。

【００２６】１９９８年４月１日から１９９８年４月３０日の期間には、バージョン４である配送用鍵Ｋｄが、

EMDサービスセンタ１、コンテンツプロバイダ２、ユーザホームネットワーク５を構成するレシーバ５１で利用される。

【００２７】このように、あらかじめ先の月の配送用鍵Ｋｄを配布しておくことで、仮にユーザーが１，２ヶ月まったくセンターにアクセスしていなくても、一応、コンテンツの買い取りが行え、時を見計らって、センターにアクセスして鍵を受信することができる。

【００２８】利益分配部１６は、経歴データ管理部１５から供給された、課金情報、価格情報、および取扱方針に基づき、EMDサービスセンタ１、コンテンツプロバイダ２、およびサービスプロバイダ３の利益を算出する。相互認証部１７は、コンテンツプロバイダ２、サービスプロバイダ３、およびユーザホームネットワーク５の所定の機器と後述する相互認証を実行する。

【００２９】ユーザ管理部１８は、ユーザ登録データベースを有し、ユーザホームネットワーク５の機器から登録の要求があったとき、ユーザ登録データベースを検索し、その記録内容に応じて、その機器を登録したり、または登録を拒絶する等の処理を実行する。ユーザホームネットワーク５がEMDサービスセンタ１と接続が可能な機能を有する複数の機器から構成されているとき、ユーザ管理部１８は、登録が可能か否かの判定の処理の結果に対応して、決済をする機器を指定し、さらに、コンテンツの利用条件を規定した登録リストをユーザホームネットワーク５の所定の機器に送信する。

【００３０】図７に示すユーザ登録データベースの例は、ユーザホームネットワーク５の機器の機器固有の６４ビットからなるID（Identification Data）を記録し、そのIDに対応して（すなわち、そのIDを有する機器毎に）、決済処理が可能か否か、登録が可能か否か、EMDサービスセンタ１と接続が可能か否か等の情報を記録する。ユーザ登録データベースに記録された登録が可能か否かの情報は、決済機関（例えば、銀行）、またはサービスプロバイダ３などから供給される料金の未払い、不正処理等の情報を基に、所定の時間間隔で更新される。登録が不可と記録されたIDを有する機器の登録の要求に対して、ユーザ管理部１８は、その登録を拒否し、登録を拒否された機器は、以後、このシステムのコンテンツを利用できない。

【００３１】ユーザ登録データベースに記録された決済処理が可能か否かの情報は、その機器が、決済可能か否かを示す。ユーザホームネットワーク５が、コンテンツの再生またはコピーなどの利用が可能な複数の機器で構成されているとき、その中の決済処理が可能である１台の機器は、EMDサービスセンタ１に、ユーザホームネットワーク５のEMDサービスセンタ１に登録されている全ての機器の、課金情報、価格情報、および取扱方針を出力する。ユーザ登録データベースに記録されたEMDサービスセンタ１と接続が可能か否かの情報は、その機器が、EMDサービスセンタ１と接続が可能であるか否かを示し、接続ができないと記録された機器は、ユーザホームネットワーク５の他の機器を介して、EMDサービスセンタ１に、課金情報等を出力する。

【００３２】また、ユーザ管理部１８は、ユーザホームネットワーク５の機器から課金情報、価格情報、および取扱方針が供給され、その情報を経歴データ管理部１５に出力し、さらに、所定の処理（タイミング）で、ユーザホームネットワーク５の機器に、配送用鍵Ｋｄを供給する。

【００３３】課金請求部１９は、経歴データ管理部１５から供給された、課金情報、価格情報、および取扱方針に基づき、ユーザへの課金を算出し、その結果を、出納部２０に供給する。出納部２０は、ユーザ、コンテンツプロバイダ２、およびサービスプロバイダ３への出金、徴収すべき利用料金の金額を基に、図示せぬ外部の銀行等と通信し、決算処理を実行する。監査部２１は、ユーザホームネットワーク５の機器から供給された課金情報、価格情報、および取扱方針の正当性（すなわち、不正をしていないか）を監査する。

【００３４】図８は、コンテンツプロバイダ２の機能の構成を示すブロック図である。コンテンツサーバ３１は、ユーザに供給するコンテンツを記憶し、ウォータマーク付加部３２に供給する。ウォータマーク付加部３２は、コンテンツサーバ３１から供給されたコンテンツにウォータマークを付加し、圧縮部３３に供給する。圧縮部３３は、ウォータマーク付加部３２から供給されたコンテンツを、ATRAC2(Adaptive Transform Acoustic Coding 2)（商標）等の方式で圧縮し、暗号化部３４に供給する。暗号化部３４は、圧縮部３３で圧縮されたコンテンツを、乱数発生部３５から供給された乱数を鍵（以下、この乱数をコンテンツ鍵Ｋｃｏと称する）として、DES(Data Encryption Standard)などの共通鍵暗号方式で暗号化し、その結果をセキュアコンテナ作成部３８に出力する。

【００３５】乱数発生部３５は、コンテンツ鍵Ｋｃｏとなる所定のビット数の乱数を暗号化部３４および暗号化部３６に供給する。暗号化部３６は、コンテンツ鍵ＫｃｏをEMDサービスセンタ１から供給された配送用鍵Ｋｄを使用して、DESなどの共通鍵暗号方式で暗号化し、その結果をセキュアコンテナ作成部３８に出力する。

【００３６】DESは、５６ビットの共通鍵を用い、平文の６４ビットを１ブロックとして処理する暗号方式である。DESの処理は、平文を撹拌し、暗号文に変換する部分（データ撹拌部）と、データ撹拌部で使用する鍵（拡大鍵）を共通鍵から生成する部分（鍵処理部）からなる。DESのすべてのアルゴリズムは公開されているので、ここでは、データ撹拌部の基本的な処理を簡単に説明する。

【００３７】まず、平文の６４ビットは、上位３２ビッ

トのH_0、および下位３２ビットのL_0に分割される。鍵処理部から供給された４８ビットの拡大鍵K_i、および下位３２ビットのL_0を入力とし、下位３２ビットのL_0を撹拌したＦ関数の出力が算出される。Ｆ関数は、数値を所定の規則で置き換える「換字」およびビット位置を所定の規則で入れ替える「転置」の２種類の基本変換から構成されている。次に、上位３２ビットのH_0と、Ｆ関数の出力が排他的論理和され、その結果はL_1とされる。L_0は、H_1とされる。

【００３８】上位３２ビットのH_0および下位３２ビットのL_0を基に、以上の処理を１６回繰り返し、得られた上位３２ビットのH_{16}および下位３２ビットのL_{16}が暗号文として出力される。復号は、暗号化に使用した共通鍵を用いて、上記の手順を逆にたどることで実現される。

【００３９】ポリシー記憶部３７は、コンテンツの取扱方針（ポリシー）を記憶し、暗号化されるコンテンツに対応して、取扱方針をセキュアコンテナ作成部３８に出力する。セキュアコンテナ作成部３８は、暗号化されたコンテンツ、暗号化されたコンテンツ鍵Ｋｃｏ、取扱方針、並びに暗号化されたコンテンツ、暗号化されたコンテンツ鍵Ｋｃｏ、および取扱方針のハッシュ値をとり作成された署名、さらにコンテンツプロバイダ２の公開鍵Ｋｐｃｐを含む証明書から構成されるコンテンツプロバイダセキュアコンテナを作成し、サービスプロバイダ３に供給する。相互認証部３９は、EMDサービスセンタ１から配送用鍵Ｋｄの供給を受けるのに先立ち、EMDサービスセンタ１と相互認証し、また、サービスプロバイダ３へのコンテンツプロバイダセキュアコンテナの送信に先立ち、サービスプロバイダ３と相互認証する。

【００４０】署名は、データまたは後述する証明書に付け、改竄のチェックおよび作成者認証をするためのデータであり、送信したいデータを基にハッシュ関数でハッシュ値をとり、これを公開鍵暗号の秘密鍵で暗号化して作成される。

【００４１】ハッシュ関数および署名の照合について説明する。ハッシュ関数は、送信したい所定のデータを入力とし、所定のビット長のデータに圧縮し、ハッシュ値として出力する関数である。ハッシュ関数は、ハッシュ値（出力）から入力を予測することが難しく、ハッシュ関数に入力されたデータの１ビットが変化したとき、ハッシュ値の多くのビットが変化し、また、同一のハッシュ値を持つ入力データを探し出すことが困難である特徴を有する。

【００４２】署名とデータを受信した受信者は、署名を公開鍵暗号の公開鍵で復号し、その結果（ハッシュ値）を得る。さらに受信されたデータのハッシュ値が計算され、計算されたハッシュ値と、署名を復号して得られたハッシュ値とが、等しいか否かが判定される。送信されたデータのハッシュ値と復号したハッシュ値が等しいと判定された場合、受信したデータは改竄されておらず、公開鍵に対応した秘密鍵を保持する送信者から送信されたデータであることがわかる。署名のハッシュ関数としては、MD4, MD5, SHA-1などが用いられる。

【００４３】次に公開鍵暗号について説明する。暗号化および復号で同一の鍵（共通鍵）を使用する共通鍵暗号方式に対し、公開鍵暗号方式は、暗号化に使用する鍵と復号するときの鍵が異なる。公開鍵暗号を用いる場合、鍵の一方を公開しても他方を秘密に保つことができ、公開しても良い鍵は、公開鍵と称され、他方の秘密に保つ鍵は、秘密鍵と称される。

【００４４】公開鍵暗号の中で代表的なRSA (Rivest-Shamir-Adleman) 暗号を、簡単に説明する。まず、２つの十分に大きな素数であるpおよびqを求め、さらにpとqの積であるｎを求める。(p-1)と(q-1)の最小公倍数Lを算出し、更に、３以上L未満で、かつ、Ｌと互いに素な数eを求める（すなわち、eとLを共通に割り切れる数は、１のみである）。

【００４５】次に、Lを法とする乗算に関するeの乗法逆元dを求める。すなわち、d, e、およびLの間には、ed=1 mod Lが成立し、dはユークリッドの互除法で算出できる。このとき、nとeが公開鍵とされ、p,q,およびdが、秘密鍵とされる。

【００４６】暗号文Cは、平文Mから、式（１）の処理で算出される。

$$C=M^e \bmod n \quad (1)$$

【００４７】暗号文Cは、式（２）の処理で平文Mに、復号される。

$$M=C^d \bmod n \quad (2)$$

【００４８】証明は省略するが、RSA暗号で平文を暗号文に変換して、それが復号できるのは、フェルマーの小定理に根拠をおいており、式（３）が成立するからである。

$$M=C^d=(M^e)^d=M^{(ed)} \bmod n \quad (3)$$

【００４９】秘密鍵pとqを知っているならば、公開鍵eから秘密鍵dは算出できるが、公開鍵nの素因数分解が計算量的に困難な程度に公開鍵nの桁数を大きくすれば、公開鍵nを知るだけでは、公開鍵eから秘密鍵dは計算できず、復号できない。以上のように、RSA暗号では、暗号化に使用する鍵と復号するときの鍵を、異なる鍵とすることができる。

【００５０】また、公開鍵暗号の他の例である楕円曲線暗号についても、簡単に説明する。楕円曲線$y^2=x^3+ax+b$上の、ある点をBとする。楕円曲線上の点の加算を定義し、nBは、Bをn回加算した結果を表す。同様に、減算も定義する。BとnBからnを算出することは、困難であることが証明されている。BとnBを公開鍵とし、nを秘密鍵とする。乱数rを用いて、暗号文C1およびC2は、平文Mから、公開鍵で式（４）および式（５）の処理で算出される。

C1=M+rnB　（４）
C2=rB　（５）
【００５１】暗号文C1およびC2は、式（６）の処理で平文Mに、復号される。
M=C1-nC2　（６）
【００５２】復号できるのは、秘密鍵nを有するものだけである。以上のように、RSA暗号と同様に、楕円曲線暗号でも、暗号化に使用する鍵と復号するときの鍵を、異なる鍵とすることができる。
【００５３】図９は、サービスプロバイダ３の機能の構成を示すブロック図である。コンテンツサーバ４１は、コンテンツプロバイダ２から供給された、暗号化されているコンテンツを記憶し、セキュアコンテナ作成部４４に供給する。値付け部４２は、コンテンツに対応した取扱方針を基に、価格情報を作成し、セキュアコンテナ作成部４４に供給する。ポリシー記憶部４３は、コンテンツプロバイダ２から供給された、コンテンツの取扱方針を記憶し、セキュアコンテナ作成部４４に供給する。相互認証部４５は、コンテンツプロバイダ２からコンテンツプロバイダセキュアコンテナの供給を受け取るのに先立ち、コンテンツプロバイダ２と相互認証し、また、ユーザホームネットワーク５へのサービスプロバイダセキュアコンテナの送信に先立ち、ユーザホームネットワーク５と相互認証する。また、コンテンツプロバイダ２が取扱方針を配送用鍵Ｋｄで暗号化して供給する場合、相互認証部４５は、EMDサービスセンタ１から配送用鍵Ｋｄの供給を受け付けるのに先立ち、EMDサービスセンタ１と相互認証する。
【００５４】図１０は、ユーザホームネットワーク５の構成を示すブロック図である。レシーバ５１は、ネットワーク４を介して、サービスプロバイダ３からコンテンツを含んだサービスプロバイダセキュアコンテナを受信し、コンテンツを復号および伸張し、再生する。
【００５５】通信部６１は、ネットワーク４を介してサービスプロバイダ３、またはEMDサービスセンタ１と通信し、所定の情報を受信し、または送信する。SAM(Secure Application Module)６２は、サービスプロバイダ３、またはEMDサービスセンタ１と相互認証し、コンテンツの暗号を復号し、またはコンテンツを暗号化し、さらに配送用鍵Ｋｄ等を記憶する。伸張部６３は、コンテンツの暗号を復号し、ATRAC2方式で伸張し、さらに所定のウォータマークをコンテンツに挿入する。IC（Integrated Circuit）カードインターフェース６４は、SAM６２からの信号を所定の形式に変更し、レシーバ５１に装着されたICカード５５に出力し、また、ICカード５５からの信号を所定の形式に変更し、SAM６２に出力する。
【００５６】サービスプロバイダ３、またはEMDサービスセンタ１と相互認証し、課金処理を実行し、コンテンツ鍵Ｋｃｏを復号および暗号化し、さらに使用許諾条件情報等の所定のデータを記憶するSAM６２は、相互認証モジュール７１、課金モジュール７２、記憶モジュール７３、および復号／暗号化モジュール７４から構成される。このSAM６２は、シングルチップの暗号処理専用ICで構成され、多層構造を有し、その内部のメモリセルはアルミニウム層等のダミー層に挟まれ、また、動作する電圧または周波数の幅が狭い等、外部から不正にデータが読み出し難い特性（耐タンパー性）を有する。
【００５７】相互認証モジュール７１は、サービスプロバイダ３、またはEMDサービスセンタ１との相互認証を実行し、必要に応じて、一時鍵Ｋｔｅｍｐ（セッション鍵）を復号／暗号化モジュール７４に供給する。課金処理モジュール７２は、サービスプロバイダ３から受信したサービスプロバイダセキュアコンテナに含まれる取扱方針および価格情報（並びに、場合によっては、取扱制御情報）から、使用許諾条件情報および課金情報を生成し、記憶モジュール７３またはHDD(Hard DiskDrive)５２に出力する。記憶モジュール７３は、課金処理モジュール７２または復号／暗号化モジュール７４から供給された課金情報、および配送用鍵Ｋｄ等のデータを記憶し、他の機能ブロックが所定の処理を実行するとき、配送用鍵Ｋｄ等のデータを供給する。
【００５８】復号／暗号化モジュール７４は、復号ユニット９１、乱数発生ユニット９２、および暗号化ユニット９３から構成される。復号ユニット９１は、暗号化されたコンテンツ鍵Ｋｃｏを配送用鍵Ｋｄで復号し、暗号化ユニット９３に出力する。乱数発生ユニット９２は、所定の桁数の乱数を発生し、保存用鍵Ｋｓａｖｅとして暗号化ユニット９３および記憶モジュール７３に出力する。ただし、一度生成して保持している場合、生成の必要はない。暗号化ユニット９３は、復号されたコンテンツ鍵Ｋｃｏを、再度、保存用鍵Ｋｓａｖｅで暗号化し、HDD５２に出力する。暗号化ユニット９３は、コンテンツ鍵Ｋｃｏを伸張部６３に送信するとき、コンテンツ鍵Ｋｃｏを一時鍵Ｋｔｅｍｐで暗号化する。
【００５９】コンテンツを復号し、伸張し、所定のウォータマークを付加する伸張部６３は、相互認証モジュール７５、復号モジュール７６、復号モジュール７７、伸張モジュール７８、およびウォータマーク付加モジュール７９から構成される。相互認証モジュール７５は、SAM６２と相互認証し、一時鍵Ｋｔｅｍｐを復号モジュール７６に出力する。復号モジュール７６は、記憶モジュール７３から出力され、一時鍵Ｋｔｅｍｐで暗号化されたコンテンツ鍵Ｋｃｏを一時鍵Ｋｔｅｍｐで復号し、復号モジュール７７に出力する。復号モジュール７７は、HDD５２に記録されたコンテンツをコンテンツ鍵Ｋｃｏで復号し、伸張モジュール７８に出力する。伸張モジュール７８は、復号されたコンテンツを、更にATRAC2等の方式で伸張し、ウォータマーク付加モジュール７９に出力する。ウォータマーク付加モジュール７９は、コンテンツにレシーバ５１を特定する所定のウォータマークを

挿入し、レコーダ５３に出力したり、図示せぬスピーカに出力し、音楽を再生する。

【００６０】HDD５２は、サービスプロバイダ３から供給されたコンテンツを記録する。装着された光ディスク（図示せず）にサービスプロバイダ３から供給されたコンテンツを記録し、再生するレコーダ５３は、記録再生部６５、SAM６６、および伸張部６７から構成される。記録再生部６５は、光ディスクが装着され、その光ディスクにコンテンツを記録し、再生する。SAM６６は、SAM６２と同じ機能を有し、その説明は省略する。伸張部６７は、伸張部６３と同じ機能を有し、その説明は省略する。MD(Mini Disk:商標)ドライブ５４は、装着された図示せぬMDにサービスプロバイダ３から供給されたコンテンツを記録し、再生する。

【００６１】ICカード５５は、レシーバ５１に装着され、記憶モジュール７３に記憶された配送用鍵Ｋｄおよび機器のIDなどの所定のデータを記憶する。例えば、新たなレシーバ５１を購入し、今まで使用していたレシーバ５１と入れ替えて使用する場合、まず、ユーザは、ICカード５５に、今まで使用していたレシーバ５１の記憶モジュール７３に記憶されていた配送用鍵Ｋｄなどの所定のデータを記憶させる。次に、ユーザは、そのICカード５５を新たなレシーバ５１に装着し、そのレシーバ５１を操作して、EMDサービスセンタ１のユーザ管理部１８にその新たなレシーバ５１を登録する。EMDサービスセンタ１のユーザ管理部１８は、ICカード５５に記憶されていたデータ（今まで使用していたレシーバ５１のIDなど）を基に、ユーザ管理部１８が保持しているデータベースから、ユーザの氏名、使用料の払い込みに使用するクレジットカードの番号などのデータを検索し、そのデータを基に、登録の処理を実行するので、ユーザは、面倒なデータを入力する必要がない。ICカード５５は、相互認証モジュール８０および記憶モジュール８１で構成される。相互認証モジュール８０は、SAM６２と相互認証する。記憶モジュール８１は、ICカードインターフェース６４を介して、SAM６２から供給されたデータを記憶し、記憶したデータをSAM６２に出力する。

【００６２】図１１は、ユーザホームネットワーク５の他の構成例を示すブロック図である。この構成のレシーバ５１およびレコーダ５３は、図１０に示した伸張部６３および伸張部６７を省略した構成を有する。その代わり、レコーダ５３に接続されているデコーダ５６が、伸張部６３または伸張部６７と同じ機能を有する。その他の構成は、図１０における場合と同様である。

【００６３】コンテンツを復号し、伸張し、ウォータマークを付加するデコーダ５６は、相互認証モジュール１０１、復号モジュール１０２、復号モジュール１０３、伸張モジュール１０４、およびウォータマーク付加モジュール１０５から構成される。相互認証モジュール１０１は、SAM６２またはSAM６６と相互認証し、一時鍵Ｋｔｅｍｐを復号モジュール１０２に出力する。復号モジュール１０２は、SAM６２から出力され、一時鍵Ｋｔｅｍｐで暗号化されたコンテンツ鍵Ｋｃｏを一時鍵Ｋｔｅｍｐで復号し、復号モジュール１０３に出力する。復号モジュール１０３は、HDD５２に記録されたコンテンツをコンテンツ鍵Ｋｃｏで復号し、伸張モジュール１０４に出力する。伸張モジュール１０４は、復号されたコンテンツを、更にATRAC2等の方式で伸張し、ウォータマーク付加モジュール１０５に出力する。ウォータマーク付加モジュール１０５は、コンテンツにデコーダ５６を特定する所定のウォータマークを挿入し、レコーダ５３に出力したり、図示せぬスピーカに出力し、音楽を再生する。

【００６４】図１２は、EMDサービスセンタ１、コンテンツプロバイダ２、サービスプロバイダ３、およびユーザホームネットワーク５の間で送受信される情報を説明する図である。コンテンツプロバイダ２は、暗号化されたコンテンツ、暗号化されたコンテンツ鍵Ｋｃｏ、取扱方針、および署名をコンテンツプロバイダセキュアコンテナ（その詳細は図１３を参照して後述する）に格納し、さらにコンテンツプロバイダセキュアコンテナにコンテンツプロバイダ２の証明書（その詳細は図１４を参照して後述する）を付して、サービスプロバイダ３に送信する。コンテンツプロバイダ２はまた、取扱方針、および署名にコンテンツプロバイダ２の証明書を付して、EMDサービスセンタ１に送信する。

【００６５】サービスプロバイダ３は、受信したコンテンツプロバイダセキュアコンテナに含まれる取扱方針を基に価格情報を生成し、暗号化されたコンテンツ、暗号化されたコンテンツ鍵Ｋｃｏ、取扱方針、価格情報、および署名をサービスプロバイダセキュアコンテナ（その詳細は図１５を参照して後述する）に格納し、さらにサービスプロバイダセキュアコンテナにサービスプロバイダ３の証明書（その詳細は図１６を参照して後述する）を付して、ユーザホームネットワーク５に送信する。サービスプロバイダ３はまた、価格情報、および署名にサービスプロバイダ３の証明書を付して、EMDサービスセンタ１に送信する。

【００６６】ユーザホームネットワーク５は、受信したサービスプロバイダセキュアコンテナに含まれる取扱方針から使用許諾情報を生成し、使用許諾情報に沿って、コンテンツを利用する。ユーザホームネットワーク５において、コンテンツ鍵Ｋｃｏが復号されると、課金情報が生成される。課金情報は、所定のタイミングで、暗号化され、取扱方針と共に署名が付され、EMDサービスセンタ１に送信される。

【００６７】EMDサービスセンタ１は、課金情報および取扱方針を基に使用料金を算出し、またEMDサービスセンタ１、コンテンツプロバイダ２、およびサービスプロバイダ３それぞれの利益を算出する。EMDサービスセン

タ１は、さらに、コンテンツプロバイダ２から受信した取扱方針、サービスプロバイダ３から受信した価格情報、並びにユーザホームネットワーク５から受信した課金情報および取扱方針を比較し、サービスプロバイダ３またはユーザホームネットワーク５で取扱方針の改竄または不正な価格の付加等の不正がなかったか否かを監査する。

【００６８】図１３は、コンテンツプロバイダセキュアコンテナを説明する図である。コンテンツプロバイダセキュアコンテナは、コンテンツ鍵Ｋｃｏで暗号化されたコンテンツ、配送用鍵Ｋｄで暗号化されたコンテンツ鍵Ｋｃｏ、取扱方針、および署名を含む。署名は、コンテンツ鍵Ｋｃｏで暗号化されたコンテンツ、配送用鍵Ｋｄで暗号化されたコンテンツ鍵Ｋｃｏ、および取扱方針にハッシュ関数を適用して生成されたハッシュ値を、コンテンツプロバイダ２の秘密鍵Ｋｓｃｐで暗号化したデータである。

【００６９】図１４は、コンテンツプロバイダ２の証明書を説明する図である。コンテンツプロバイダ２の証明書は、証明書のバージョン番号、認証局がコンテンツプロバイダ２に対し割り付ける証明書の通し番号、署名に用いたアルゴリズムおよびパラメータ、認証局の名前、証明書の有効期限、コンテンツプロバイダ２の名前、コンテンツプロバイダの公開鍵Ｋｐｃｐ、並びに署名を含む。署名は、証明書のバージョン番号、認証局がコンテンツプロバイダ２に対し割り付ける証明書の通し番号、署名に用いたアルゴリズムおよびパラメータ、認証局の名前、証明書の有効期限、コンテンツプロバイダ２の名前、並びにコンテンツプロバイダの公開鍵Ｋｐｃｐにハッシュ関数を適用して生成されたハッシュ値を、認証局の秘密鍵Ｋｓｃａで暗号化したデータである。

【００７０】図１５は、サービスプロバイダセキュアコンテナを説明する図である。サービスプロバイダセキュアコンテナは、コンテンツ鍵Ｋｃｏで暗号化されたコンテンツ、配送用鍵Ｋｄで暗号化されたコンテンツ鍵Ｋｃｏ、取扱方針、価格情報、および署名を含む。署名は、コンテンツ鍵Ｋｃｏで暗号化されたコンテンツ、配送用鍵Ｋｄで暗号化されたコンテンツ鍵Ｋｃｏ、取扱方針、および価格情報にハッシュ関数を適用して生成されたハッシュ値を、サービスプロバイダ３の秘密鍵Ｋｓｓｐで暗号化したデータである。

【００７１】図１６は、サービスプロバイダ３の証明書を説明する図である。サービスプロバイダ３の証明書は、証明書のバージョン番号、認証局がサービスプロバイダ３に対し割り付ける証明書の通し番号、署名に用いたアルゴリズムおよびパラメータ、認証局の名前、証明書の有効期限、サービスプロバイダ３の名前、サービスプロバイダの公開鍵Ｋｐｓｐ、並びに署名を含む。署名は、証明書のバージョン番号、認証局がサービスプロバイダ３に対し割り付ける証明書の通し番号、署名に用いたアルゴリズムおよびパラメータ、認証局の名前、証明書の有効期限、サービスプロバイダ３の名前、サービスプロバイダの公開鍵Ｋｐｓｐにハッシュ関数を適用して生成されたハッシュ値を、認証局の秘密鍵Ｋｓｃａで暗号化したデータである。

【００７２】図１７は、取扱方針、価格情報、および使用許諾条件情報を示す図である。コンテンツプロバイダ２が有する取扱方針（図１７（Ａ））は、コンテンツ毎に用意され、ユーザホームネットワーク５が利用可能な利用内容を示す。例えば、図１７（Ａ）の取り扱い方針は、ユーザホームネットワーク５がそのコンテンツを再生およびマルチコピーすることは許可するが、シングルコピーは許可しないことを示す。

【００７３】図１８は、シングルコピーおよびマルチコピーを説明する図である。マルチコピーは、使用許諾条件情報においてコピー許可が与えられているコンテンツに対し、その使用許諾条件を購入した場合において、そのコンテンツから、複数のコピーを作成することを言う。ただし、図１８（Ａ）に示すように、コピーを更にコピーすることはできない（許されない）。シングルコピーは、使用許諾条件情報においてコピー許可が与えられているコンテンツに対し、その使用許諾条件を購入した場合において、そのコンテンツから、ただ１つのコピーを作成することを言う。シングルコピーの場合も、図１８（Ｂ）に示すように、コピーを更にコピーすることはできない（許されない）。

【００７４】サービスプロバイダ３は、図１７（Ｂ）に示すように、コンテンツプロバイダ２からの取扱方針（図１７（Ａ））に価格情報を加える。例えば、図１７（Ｂ）の価格情報は、そのコンテンツを再生して利用するときの料金が１５０円で、マルチコピーして利用するときの利用料金が８０円であることを示す。図１７には、例示しないが、シングルコピーの価格情報は、コピーの１回当たりの使用料金を表し、例えば、３回のコピーの利用では、シングルコピーの使用料金の３倍の料金を支払う。マルチコピーまたはシングルコピーが許可されるコンテンツは、使用許諾条件情報においてコピー許可が与えられているコンテンツに対し、その使用許諾条件を購入した場合における、そのコンテンツに限られる。

【００７５】ユーザホームネットワーク５は、サービスプロバイダ３から供給される取扱方針が示すコンテンツの利用可能な利用内容（図１７（Ｂ））から、ユーザが選択した、利用内容を示す使用許諾条件情報（図１７（Ｃ））を記憶する。例えば、図１７（Ｃ）の使用許諾条件情報は、そのコンテンツを再生して使用することができ、シングルコピーおよびマルチコピーができないことを示す。

【００７６】図１９は、図１７の例と比較してコンテンツプロバイダ２が取扱方針に利益分配の情報を加え、サ

ービスプロバイダ３が価格情報に利益分配の情報を加える場合の、取扱方針および価格情報を説明する図である。図１７に示す例に対して、図１９の例では、コンテンツプロバイダ２の利益が、コンテンツを再生して利用するとき７０円で、マルチコピーして利用するとき４０円であることを示す情報が、追加されている（図１９（Ａ））。更に、利益分配情報として、サービスプロバイダ３の利益が、コンテンツを再生して利用するとき６０円で、マルチコピーして利用するとき３０円であることが、追加されている（図１９（Ｂ））。価格は、図１７（Ａ）における場合と同様に、再生が１５０円、マルチコピーが４０円とされている。価格（例えば１５０円）からコンテンツプロバイダ２の利益（例えば７０円）およびサービスプロバイダ３の利益（例えば６０円）を差し引いた金額（例えば２０円）が、EMDサービスセンタ１の利益である。EMDサービスセンタ１は、ユーザホームネットワーク５のコンテンツの利用結果を示す課金情報（図１９（Ｃ））とともに、ユーザホームネットワーク５を介して、取扱方針、利益分配率、および価格情報を得ることで、コンテンツプロバイダ２、サービスプロバイダ３、およびEMDサービスセンタ１のそれぞれの利益を算出できる。

【００７７】図２０は、コンテンツの再生の利用に、複数の形態が設定されているときの取扱方針、価格情報、および使用許諾条件情報を説明する図である。図２０（Ａ）の例では、サービスプロバイダ３において、取扱方針および価格情報として、コンテンツの再生利用に、制限のない再生、回数制限（この例の場合、５回）のある再生、および期日制限（この例の場合、１９９８年１２月３１日まで）のある再生が設定されている。ユーザが、５回の回数制限のある再生を選択して、コンテンツを利用する場合、コンテンツを受け取り、まだ１度も再生していない状態では、図２０（Ｂ）に示すように、ユーザホームネットワーク５の使用許諾条件情報の回数制限に対応する値には、”５”が記録されている。この回数制限に対応する値は、ユーザホームネットワーク５において、コンテンツが再生（利用）される度にデクリメントされ、例えば、３回再生された後、その値は、図２０（Ｃ）に示すように”２”とされる。回数制限に対応する値が、”０”となった場合、ユーザホームネットワーク５は、それ以上、そのコンテンツを再生して利用することができない。

【００７８】図２１は、EMDサービスセンタ１、コンテンツプロバイダ２、サービスプロバイダ３、およびユーザホームネットワーク５の間で送受信される情報の他の例を説明する図である。図１２に示した例に対して、図２１の例では、サービスプロバイダ３は、コンテンツプロバイダ２からの取扱方針を基に取扱制御情報を作成する。取扱制御情報は、コンテンツなどと共にサービスプロバイダセキュアコンテナに格納され、ユーザホームネットワーク５に送信され、EMDサービスセンタ１にも送信される。取扱制御情報は、更に、課金情報および取扱方針と共にユーザホームネットワーク５からEMDサービスセンタ１に送信される。

【００７９】図２２は、図２１の例の場合のサービスプロバイダセキュアコンテナを説明する図である。サービスプロバイダセキュアコンテナは、コンテンツ鍵Ｋｃｏで暗号化されたコンテンツ、配送用鍵Ｋｄで暗号化されたコンテンツ鍵Ｋｃｏ、取扱方針、取扱制御情報、価格情報、および署名を含む。署名は、コンテンツ鍵Ｋｃｏで暗号化されたコンテンツ、配送用鍵Ｋｄで暗号化されたコンテンツ鍵Ｋｃｏ、取扱方針、取扱制御情報、および価格情報にハッシュ関数を適用して生成されたハッシュ値を、サービスプロバイダ３の秘密鍵Ｋｓｓｐで暗号化したデータである。

【００８０】図２３は、図２１の例の場合における、取扱方針、取扱制御情報、価格情報、及び使用許諾条件の構成を示す図である。図２３に示す例の場合、コンテンツプロバイダ２の取扱方針（図２３（Ａ））は、そのまま価格情報を付しても、取扱方針と対比して価格情報を参照できる形式を有しない。そこで、サービスプロバイダ３は、その取扱方針を基に、価格情報と対比して価格情報を参照できる形式を有する取扱制御情報を生成し、それに価格情報を付して、ユーザホームネットワーク５に送信する（図２３（Ｂ））。ユーザホームネットワークでは、送信を受けた情報から使用許諾条件情報（図２３（Ｃ））を生成する。図２３のコンテンツプロバイダ２は、図１２の場合に比較し、より小さいデータ量の取扱方針を記録すればよい利点がある。

【００８１】図２４は、EMDサービスセンタ１、コンテンツプロバイダ２、サービスプロバイダ３、およびユーザホームネットワーク５の間で送受信されるコンテンツおよびコンテンツに付随する情報のさらに他の構成を説明する図である。図２１に示した例に対して、図２４の例では、取扱方針、取扱制御情報、価格情報、および課金情報は、公開鍵暗号により暗号化され、送信される。図２４のシステムは、図２１の例の場合に比較して、システムの外部からの攻撃に対し、安全性が向上する。

【００８２】図２５は、図２４の例の場合のコンテンツプロバイダセキュアコンテナを説明する図である。コンテンツプロバイダセキュアコンテナは、コンテンツ鍵Ｋｃｏで暗号化されたコンテンツ、配送用鍵Ｋｄで暗号化されたコンテンツ鍵Ｋｃｏ、配送用鍵Ｋｄで暗号化された取扱方針、および署名を含む。署名は、コンテンツ鍵Ｋｃｏで暗号化されたコンテンツ、配送用鍵Ｋｄで暗号化されたコンテンツ鍵Ｋｃｏ、および配送用鍵Ｋｄで暗号化された取扱方針にハッシュ関数を適用して生成されたハッシュ値を、コンテンツプロバイダ２の秘密鍵Ｋｓｃｐで暗号化したデータである。

【００８３】図２６は、図２４の例の場合のサービスプ

19

ロバイダセキュアコンテナを説明する図である。サービスプロバイダセキュアコンテナは、コンテンツ鍵Ｋｃｏで暗号化されたコンテンツ、配送用鍵Ｋｄで暗号化されたコンテンツ鍵Ｋｃｏ、配送用鍵Ｋｄで暗号化された取扱方針、配送用鍵Ｋｄで暗号化された取扱制御情報、配送用鍵Ｋｄで暗号化された価格情報、および署名を含む。署名は、コンテンツ鍵Ｋｃｏで暗号化されたコンテンツ、配送用鍵Ｋｄで暗号化されたコンテンツ鍵Ｋｃｏ、配送用鍵Ｋｄで暗号化された取扱方針、配送用鍵Ｋｄで暗号化された取扱制御情報、および配送用鍵Ｋｄで暗号化された価格情報にハッシュ関数を適用して生成されたハッシュ値を、サービスプロバイダ３の秘密鍵Ｋｓｓｐで暗号化したデータである。

【００８４】図２７は、EMDサービスセンタ１が、コンテンツプロバイダ２、サービスプロバイダ３、およびユーザホームネットワーク５から、決算処理に必要なデータを収集する他の動作を説明する図である。コンテンツプロバイダ２は、EMDサービスセンタ１に、コンテンツプロバイダ２の名前、コンテンツID、コンテンツIDに対応する権利団体の利益、およびコンテンツプロバイダ２の銀行口座番号などのデータからなるコンテンツプロバイダ登録データを送信し、EMDサービスセンタ１のコンテンツプロバイダ管理部１２は、コンテンツプロバイダ登録データを受信する。EMDサービスセンタ１のコンテンツプロバイダ管理部１２は、コンテンツプロバイダ登録データを受信したとき、コンテンツプロバイダIDを生成し、コンテンツプロバイダIDとともにコンテンツプロバイダ登録データを利益配分データベースに登録し、コンテンツプロバイダIDをコンテンツプロバイダ２に送信する。コンテンツプロバイダ２は、コンテンツプロバイダIDを受信し、記憶する。

【００８５】サービスプロバイダ３は、EMDサービスセンタ１にサービスプロバイダ３の名前、コンテンツID、およびサービスプロバイダ３の銀行口座番号などのデータからなるサービスプロバイダ登録データを送信し、EMDサービスセンタ１のサービスプロバイダ管理部１１は、サービスプロバイダ登録データを受信する。EMDサービスセンタ１のサービスプロバイダ管理部１１は、サービスプロバイダ登録データを受信したとき、サービスプロバイダIDを生成し、サービスプロバイダIDをサービスプロバイダ３に送信する。サービスプロバイダ３は、コンテンツプロバイダIDを受信し、記憶する。

【００８６】ユーザホームネットワーク５は、EMDサービスセンタ１にユーザの名前、ユーザの銀行口座番号などのデータからなるユーザ登録データを送信し、EMDサービスセンタ１のユーザ管理部１８は、ユーザ登録データを受信する。EMDサービスセンタ１のユーザ管理部１８は、ユーザ登録データの受信により、ユーザIDを生成し、ユーザIDとともにユーザ登録データを記憶し、ユーザIDをユーザホームネットワーク５に送信する。ユーザホームネットワーク５は、ユーザIDを受信し、記憶する。

20

【００８７】図２８は、利益配分データベースの例を示す図である。利益配分データベースは、コンテンツIDに対応する権利団体への配分が記憶されている。コンテンツIDに対応する権利団体への配分は、権利団体への、コンテンツIDに対応するコンテンツがユーザに利用されたときに発生する利益の配分の割合を示す。

【００８８】図２８に示す利益配分データベースの例において、コンテンツIDが１であるコンテンツがサービスプロバイダ３からユーザに提供された場合、権利団体には、コンテンツがユーザに利用されることによる利益の１０％が配分される。同様に、コンテンツIDが２であるコンテンツがユーザに利用されることによる利益の２０％は、権利団体に配分される。

【００８９】図２９は、EMDサービスセンタ１の利益分配部１６が記憶するコンテンツの利用料金の割引テーブルの例を示す図である。コンテンツの利用料金の割引テーブルには、コンテンツIDおよびコンテンツプロバイダIDに対応するユーザの利用料金の割引率が格納されている。割引テーブルには、割引率を、適用する期間の情報なども格納できるようになされている。

【００９０】コンテンツプロバイダIDが1であるコンテンツプロバイダ２が供給するコンテンツIDが1であるコンテンツの利用料金は、１９９８年９月から１９９８年１２月までの間、０．０２割り引かれる。コンテンツプロバイダIDが1であるコンテンツプロバイダ２が供給するコンテンツIDが2であるコンテンツの利用料金は、０．０３割り引かれる。コンテンツプロバイダIDが1であるコンテンツプロバイダ２が供給するコンテンツIDが1または2以外であるコンテンツの利用料金は、０．０１割り引かれる。コンテンツプロバイダIDが2であるコンテンツプロバイダ２が供給するコンテンツIDが3であるコンテンツの利用料金は、０．０５割り引かれる。サービスプロバイダIDが1であるサービスプロバイダ３が提供するコンテンツIDが1であるコンテンツの利用料金は、０．０３割り引かれる。サービスプロバイダIDが2であるサービスプロバイダ３が提供するコンテンツIDが4であるコンテンツの利用料金は、０．０１割り引かれる。

【００９１】図３０は、EMDサービスセンタ１の課金請求部１９が記憶する、ユーザに対するEMDサービスセンタ１の利用料金を格納するユーザ利用料金テーブルの例を示している。ユーザ利用料金テーブルの月額固定額は、ユーザがEMDサービスセンタ１に毎月支払う一定の利用料金の額を表す。変動額は、EMDサービスセンタ１特別に定めた所定の期間の月額固定額の割引率、または、コンテンツの利用料金を含めた利用料が所定の額以上である場合の月額固定額の割引率を表す。

【００９２】図３０に示すユーザ利用料金テーブルの例

において、月額固定額は、１０００円であり、１９９８年８月から１９９８年９月の間、月額固定額は、１０％割り引かれる。また、コンテンツの利用料金を含めた利用料が３０００円以上である場合、月額固定額は、５％割り引かれる。

【００９３】利益配分データベースまたは課金情報からコンテンツの利用料金が算出され、コンテンツの利用料金から割引テーブルに基づく割引額が減算され、ユーザ利用料金テーブルに格納されているEMDサービスセンタ１の利用料金が加算されて、ユーザの利用料金が、算出される。

【００９４】図３１は、EMDサービスセンタ１が、ユーザホームネットワーク５から課金情報を受信するときの動作を説明する図である。ユーザホームネットワーク５と相互認証した後、ユーザ管理部１８は、一時鍵Ｋｔｅｍｐを共有化し、鍵サーバ１４からの配送用鍵Ｋｄをこの鍵で暗号化しユーザホームネットワーク５に送信する。ユーザホームネットワーク５は、受信した配送用鍵Ｋｄを共有化した一時鍵Ｋｔｅｍｐで復号化した後、配送用鍵Ｋｄを必要に応じて更新する。また、共有化した一時鍵Ｋｔｅｍｐを用いて課金情報、および取扱方針等を暗号化し、EMDサービスセンタ１に送信する。ユーザ管理部１８はこれを受信する。ユーザ管理部１８は、受信した課金情報、および取扱方針等を共有化した一時鍵Ｋｔｅｍｐで復号化した後、経歴データ管理部１５および課金請求部１９に送信する。経歴データ管理部１５は決済を実行すると判定した場合、受信した課金情報を利益分配部１６に送信し、さらに、受信した課金情報および取扱方針等を課金請求部１９に送信する。利益分配部１６は、利益配分データベース、および割引テーブルを基に、図５７で説明する処理で、コンテンツプロバイダ２、サービスプロバイダ３、およびEMDサービスセンタ１自身に対する請求金額および支払金額を算出する。課金請求部１９は、ユーザ利用料金テーブルを基に、ユーザへの請求金額を算出し、その情報を出納部２０に送信する。出納部２０は、図示せぬ外部の銀行等と通信し、決算処理を実行する。その際、ユーザの料金の未払い等の情報があれば、それらの情報は、課金請求部１９およびユーザ管理部１８に送信され、以後のユーザの登録処理時、または配送用鍵Ｋｄの送信処理時に参照される。

【００９５】図３２は、EMDサービスセンタ１の利益分配処理の動作を説明する図である。経歴データ管理部１５は、ユーザのコンテンツの使用実績を示す課金情報、取扱方針、および価格データを利益分配部１６に送信する。利益分配部１６は、これらの情報を基に、コンテンツプロバイダ２、サービスプロバイダ３、およびEMDサービスセンタ１それぞれの利益を算出し、その結果をサービスプロバイダ管理部１１、コンテンツプロバイダ管理部１２、出納部２０、および著作権管理部１３に送信する。出納部２０は、図示せぬ外部の銀行等と通信し、決算処理を実行する。サービスプロバイダ管理部１１は、サービスプロバイダ３の利益の情報をサービスプロバイダ３に送信する。コンテンツプロバイダ管理部１２は、コンテンツプロバイダ２の利益の情報をコンテンツプロバイダ２に送信する。監査部２１は、ユーザホームネットワーク５の機器から供給された課金情報、価格情報、および取扱方針の正当性を監査する。

【００９６】図３３は、EMDサービスセンタ１の、コンテンツの利用実績の情報をJASRACに送信する処理の動作を説明する図である。経歴データ管理部１５は、ユーザのコンテンツの使用実績を示す課金情報を著作権管理部１３および利益分配部１６に送信する。利益分配部１６は、利益配分データベース、および割引テーブルを基に、図５７で説明する処理で、JASRACに対する請求金額および支払金額を算出し、その情報を出納部２０に送信する。出納部２０は、図示せぬ外部の銀行等と通信し、決算処理を実行する。著作権管理部１３は、ユーザのコンテンツの使用実績をJASRACに送信する。

【００９７】次に、EMDシステムの処理について説明する。図３４は、このシステムのコンテンツの配布および再生の処理を説明するフローチャートである。ステップＳ１１において、EMDサービスセンタ１のコンテンツプロバイダ管理部１２は、コンテンツプロバイダ２に配送用鍵Ｋｄを送信し、コンテンツプロバイダ２がこれを受信する。その処理の詳細は、図３６のフローチャートを参照して後述する。ステップＳ１２において、ユーザは、ユーザホームネットワーク５の機器（例えば、図１０のレシーバ５１）を操作し、ユーザホームネットワーク５の機器をEMDサービスセンタ１のユーザ管理部１８に登録する。この登録処理の詳細は、図４０のフローチャートを参照して後述する。ステップＳ１３において、EMDサービスセンタ１のユーザ管理部１８は、ユーザホームネットワーク５と、図３７乃至図３９に示したように相互認証した後、ユーザホームネットワーク５の機器に、配送用鍵Ｋｄを送信する。ユーザホームネットワーク５はこの鍵を受信する。この処理の詳細は、図４８のフローチャートを参照して説明する。

【００９８】ステップＳ１４において、コンテンツプロバイダ２のセキュアコンテナ作成部３８は、サービスプロバイダ３にコンテンツプロバイダセキュアコンテナを送信する。この送信処理の詳細は、図５０のフローチャートを参照して後述する。ステップＳ１５において、サービスプロバイダ３のセキュアコンテナ作成部４４は、ユーザホームネットワーク５からの要求に応じて、ネットワーク４を介して、ユーザホームネットワーク５にサービスプロバイダセキュアコンテナを送信する。この送信処理の詳細は、図５２のフローチャートを参照して後述する。ステップＳ１６において、ユーザホームネットワーク５の課金モジュール７２は、課金処理を実行する。課金処理の詳細は、図５４のフローチャートを参照

して後述する。ステップＳ１７において、ユーザは、ユーザホームネットワーク５の機器でコンテンツを再生する。再生処理の詳細は、図５５のフローチャートを参照して後述する。

【００９９】一方、コンテンツプロバイダ２が、取扱方針を暗号化して送信する場合の処理は、図３５のフローチャートで示すようになる。ステップＳ２１において、EMDサービスセンタ１のコンテンツプロバイダ管理部１２は、コンテンツプロバイダ２に配送用鍵Ｋｄを送信する。ステップＳ２２において、EMDサービスセンタ１のサービスプロバイダ管理部１１は、サービスプロバイダ３に配送用鍵Ｋｄを送信する。それ以降のステップＳ２３乃至ステップＳ２８の処理は、図３４のステップＳ１２乃至ステップＳ１７の処理と同様の処理であり、その説明は省略する。

【０１００】図３６は、図３４のステップＳ１１および図３５のステップＳ２１に対応する、EMDサービスセンタ１がコンテンツプロバイダ２へ配送用鍵Ｋｄを送信し、コンテンツプロバイダ２がこれを受信する処理の詳細を説明するフローチャートである。ステップＳ３１において、EMDサービスセンタ１の相互認証部１７は、コンテンツプロバイダ２の相互認証部３９と相互認証する。この相互認証処理の詳細は、図３７を参照して後述する。相互認証処理により、コンテンツプロバイダ２が、正当なプロバイダであることが確認されたとき、ステップＳ３２において、コンテンツプロバイダ２の暗号化部３４および暗号化部３６は、EMDサービスセンタ１のコンテンツプロバイダ管理部１２から送信された配送用鍵Ｋｄを受信する。ステップＳ３３において、コンテンツプロバイダ２の暗号化部３４は、受信した配送用鍵Ｋｄを記憶する。

【０１０１】このように、コンテンツプロバイダ２は、EMDサービスセンタ１から配送用鍵Ｋｄを受け取る。同様に、図３５に示すフローチャートの処理を行う例の場合、コンテンツプロバイダ２以外に、サービスプロバイダ３も、図３６と同様の処理で、EMDサービスセンタ１から配送用鍵Ｋｄを受け取る。

【０１０２】次に、図３６のステップＳ３１における、いわゆるなりすましがないことを確認する相互認証の処理について、１つの共通鍵を用いる（図３７）、２つの共通鍵を用いる（図３８）、および公開鍵暗号を用いる（図３９）を例として説明する。

【０１０３】図３７は、１つの共通鍵で、共通鍵暗号であるDESを用いる、コンテンツプロバイダ２の相互認証部３９とEMDサービスセンタ１の相互認証部１７との相互認証の動作を説明するフローチャートである。ステップＳ４１において、コンテンツプロバイダ２の相互認証部３９は、６４ビットの乱数Ｒ１を生成する（乱数生成部３５が生成するようにしてもよい）。ステップＳ４２において、コンテンツプロバイダ２の相互認証部３９は、DESを用いて乱数Ｒ１を、予め記憶している共通鍵Ｋｃで暗号化する（暗号化部３６で暗号化するようにしてもよい）。ステップＳ４３において、コンテンツプロバイダ２の相互認証部３９は、暗号化された乱数Ｒ１をEMDサービスセンタ１の相互認証部１７に送信する。

【０１０４】ステップＳ４４において、EMDサービスセンタ１の相互認証部１７は、受信した乱数Ｒ１を予め記憶している共通鍵Ｋｃで復号する。ステップＳ４５において、EMDサービスセンタ１の相互認証部１７は、３２ビットの乱数Ｒ２を生成する。ステップＳ４６において、EMDサービスセンタ１の相互認証部１７は、復号した６４ビットの乱数Ｒ１の下位３２ビットを乱数Ｒ２で入れ替え、連接$R1_H \| R2$を生成する。なお、ここでRi_Hは、Ｒｉの上位ビットを表し、Ａ‖Ｂは、ＡとＢの連接（ｎビットのＡの下位に、ｍビットのＢを結合して、（ｎ＋ｍ）ビットとしたもの）を表す。ステップＳ４７において、EMDサービスセンタ１の相互認証部１７は、DESを用いて$R1_H \| R2$を共通鍵Ｋｃで暗号化する。ステップＳ４８において、EMDサービスセンタ１の相互認証部１７は、暗号化した$R1_H \| R2$をコンテンツプロバイダ２に送信する。

【０１０５】ステップＳ４９において、コンテンツプロバイダ２の相互認証部３９は、受信した$R1_H \| R2$を共通鍵Ｋｃで復号する。ステップＳ５０において、コンテンツプロバイダ２の相互認証部３９は、復号した$R1_H \| R2$の上位３２ビット$R1_H$を調べ、ステップＳ４１で生成した、乱数Ｒ１の上位３２ビット$R1_H$と一致すれば、EMDサービスセンタ１が正当なセンタであることを認証する。生成した乱数$R1_H$と、受信した$R1_H$が一致しないとき、処理は終了される。両者が一致するとき、ステップＳ５１において、コンテンツプロバイダ２の相互認証部３９は、３２ビットの乱数Ｒ３を生成する。ステップＳ５２において、コンテンツプロバイダ２の相互認証部３９は、受信し、復号した３２ビットの乱数Ｒ２を上位に設定し、生成した乱数Ｒ３をその下位に設定し、連接$R2 \| R3$とする。ステップＳ５３において、コンテンツプロバイダ２の相互認証部３９は、DESを用いて連接$R2 \| R3$を共通鍵Ｋｃで暗号化する。ステップＳ５４において、コンテンツプロバイダ２の相互認証部３９は、暗号化された連接$R2 \| R3$をEMDサービスセンタ１の相互認証部１７に送信する。

【０１０６】ステップＳ５５において、EMDサービスセンタ１の相互認証部１７は、受信した連接$R2 \| R3$を共通鍵Ｋｃで復号する。ステップＳ５６において、EMDサービスセンタ１の相互認証部１７は、復号した連接$R2 \| R3$の上位３２ビットを調べ、乱数Ｒ２と一致すれば、コンテンツプロバイダ２を正当なプロバイダとして認証し、一致しなければ、不正なプロバイダとして、処理を終了する。

【０１０７】図３８は、２つの共通鍵Ｋｃ１，Ｋｃ２

25

で、共通鍵暗号であるDESを用いる、コンテンツプロバイダ２の相互認証部３９とEMDサービスセンタ１の相互認証部１７との相互認証の動作を説明するフローチャートである。ステップＳ６１において、コンテンツプロバイダ２の相互認証部３９は、６４ビットの乱数Ｒ１を生成する。ステップＳ６２において、コンテンツプロバイダ２の相互認証部３９は、DESを用いて乱数Ｒ１を予め記憶している共通鍵Ｋｃ１で暗号化する。ステップＳ６３において、コンテンツプロバイダ２の相互認証部３９は、暗号化された乱数Ｒ１をEMDサービスセンタ１に送信する。

【０１０８】ステップＳ６４において、EMDサービスセンタ１の相互認証部１７は、受信した乱数Ｒ１を予め記憶している共通鍵Ｋｃ１で復号する。ステップＳ６５において、EMDサービスセンタ１の相互認証部１７は、乱数Ｒ１を予め記憶している共通鍵Ｋｃ２で暗号化する。ステップＳ６６において、EMDサービスセンタ１の相互認証部１７は、６４ビットの乱数Ｒ２を生成する。ステップＳ６７において、EMDサービスセンタ１の相互認証部１７は、乱数Ｒ２を共通鍵Ｋｃ２で暗号化する。ステップＳ６８において、EMDサービスセンタ１の相互認証部１７は、暗号化された乱数Ｒ１および乱数Ｒ２をコンテンツプロバイダ２の相互認証部３９に送信する。

【０１０９】ステップＳ６９において、コンテンツプロバイダ２の相互認証部３９は、受信した乱数Ｒ１および乱数Ｒ２を予め記憶している共通鍵Ｋｃ２で復号する。ステップＳ７０において、コンテンツプロバイダ２の相互認証部３９は、復号した乱数Ｒ１を調べ、ステップＳ６１で生成した乱数Ｒ１（暗号化する前の乱数Ｒ１）と一致すれば、EMDサービスセンタ１を適正なセンタとして認証し、一致しなければ、不正なセンタであるとして、処理を終了する。ステップＳ７１において、コンテンツプロバイダ２の相互認証部３９は、復号して得た乱数Ｒ２を共通鍵Ｋｃ１で暗号化する。ステップＳ７２において、コンテンツプロバイダ２の相互認証部３９は、暗号化された乱数Ｒ２をEMDサービスセンタ１に送信する。

【０１１０】ステップＳ７３において、EMDサービスセンタ１の相互認証部１７は、受信した乱数Ｒ２を共通鍵Ｋｃ１で復号する。ステップＳ７４において、EMDサービスセンタ１の相互認証部１７は、復号した乱数Ｒ２が、ステップＳ６６で生成した乱数Ｒ２（暗号化する前の乱数Ｒ２）と一致すれば、コンテンツプロバイダ２を適正なプロバイダとして認証し、一致しなければ、不正なプロバイダであるとして処理を終了する。

【０１１１】図３９は、公開鍵暗号である、１６０ビット長の楕円曲線暗号を用いる、コンテンツプロバイダ２の相互認証部３９とEMDサービスセンタ１の相互認証部１７との相互認証の動作を説明するフローチャートである。ステップＳ８１において、コンテンツプロバイダ２

26

の相互認証部３９は、６４ビットの乱数Ｒ１を生成する。ステップＳ８２において、コンテンツプロバイダ２の相互認証部３９は、自分自身の公開鍵Ｋｐｃｐを含む証明書（認証局から予め取得しておいたもの）と、乱数Ｒ１をEMDサービスセンタ１の相互認証部１７に送信する。

【０１１２】ステップＳ８３において、EMDサービスセンタ１の相互認証部１７は、受信した証明書の署名（認証局の秘密鍵Ｋｓｃａで暗号化されている）を、予め取得しておいた認証局の公開鍵Ｋｐｃａで復号し、コンテンツプロバイダ２の公開鍵Ｋｐｃｐとコンテンツプロバイダ２の名前のハッシュ値を取り出すとともに、証明書に平文のまま格納されているコンテンツプロバイダ２の公開鍵Ｋｐｃｐおよびコンテンツプロバイダ２の名前を取り出す。証明書が認証局が発行した適正なものであれば、証明書の署名を復号することが可能であり、復号して得られた公開鍵Ｋｐｃｐおよびコンテンツプロバイダ２の名前のハッシュ値は、平文のまま証明書に格納されていたコンテンツプロバイダ２の公開鍵Ｋｐｃｐおよびコンテンツプロバイダ２の名前にハッシュ関数を適用して得られたハッシュ値と一致する。これにより、公開鍵Ｋｐｃｐが改竄されたものでない適正なものであることが認証される。署名を復号出来なかったり、できたとしてもハッシュ値が一致しないときには、適正な公開鍵でないか、適正なプロバイダでないことになる。この時処理は終了される。

【０１１３】適正な認証結果が得られたとき、ステップＳ８４において、EMDサービスセンタ１の相互認証部１７は、６４ビットの乱数Ｒ２を生成する。ステップＳ８５において、EMDサービスセンタ１の相互認証部１７は、乱数Ｒ１および乱数Ｒ２の連接Ｒ１‖Ｒ２を生成する。ステップＳ８６において、EMDサービスセンタ１の相互認証部１７は、連接Ｒ１‖Ｒ２を自分自身の秘密鍵Ｋｓｅｓｃで暗号化する。ステップＳ８７において、EMDサービスセンタ１の相互認証部１７は、連接Ｒ１‖Ｒ２を、ステップＳ８３で取得したコンテンツプロバイダ２の公開鍵Ｋｐｃｐで暗号化する。ステップＳ８８において、EMDサービスセンタ１の相互認証部１７は、秘密鍵Ｋｓｅｓｃで暗号化された連接Ｒ１‖Ｒ２、公開鍵Ｋｐｃｐで暗号化された連接Ｒ１‖Ｒ２、および自分自身の公開鍵Ｋｐｅｓｃを含む証明書（認証局から予め取得しておいたもの）をコンテンツプロバイダ２の相互認証部３９に送信する。

【０１１４】ステップＳ８９において、コンテンツプロバイダ２の相互認証部３９は、受信した証明書の署名を予め取得しておいた認証局の公開鍵Ｋｐｃａで復号し、正しければ証明書から公開鍵Ｋｐｅｓｃを取り出す。この場合の処理は、ステップＳ８３における場合と同様であるので、その説明は省略する。ステップＳ９０において、コンテンツプロバイダ２の相互認証部３９は、EMD

サービスセンタ１の秘密鍵Ｋｓｅｓｃで暗号化されている連接Ｒ１‖Ｒ２を、ステップＳ８９で取得した公開鍵Ｋｐｅｓｃで復号する。ステップＳ９１において、コンテンツプロバイダ２の相互認証部３９は、自分自身の公開鍵Ｋｐｃｐで暗号化されている連接Ｒ１‖Ｒ２を、自分自身の秘密鍵Ｋｓｃｐで復号する。ステップＳ９２において、コンテンツプロバイダ２の相互認証部３９は、ステップＳ９０で復号された連接Ｒ１‖Ｒ２と、ステップＳ９１で復号された連接Ｒ１‖Ｒ２を比較し、一致すればEMDサービスセンタ１を適正なものとして認証し、一致しなければ、不適正なものとして、処理を終了する。

【０１１５】適正な認証結果が得られたとき、ステップＳ９３において、コンテンツプロバイダ２の相互認証部３９は、６４ビットの乱数Ｒ３を生成する。ステップＳ９４において、コンテンツプロバイダ２の相互認証部３９は、ステップＳ９０で取得した乱数Ｒ２および生成した乱数Ｒ３の連接Ｒ２‖Ｒ３を生成する。ステップＳ９５において、コンテンツプロバイダ２の相互認証部３９は、連接Ｒ２‖Ｒ３を、ステップＳ８９で取得した公開鍵Ｋｐｅｓｃで暗号化する。ステップＳ９６において、コンテンツプロバイダ２の相互認証部３９は、暗号化した連接Ｒ２‖Ｒ３をEMDサービスセンタ１の相互認証部１７に送信する。

【０１１６】ステップＳ９７において、EMDサービスセンタ１の相互認証部１７は、暗号化された連接Ｒ２‖Ｒ３を自分自身の秘密鍵Ｋｓｅｓｃで復号する。ステップＳ９８において、EMDサービスセンタ１の相互認証部１７は、復号した乱数Ｒ２が、ステップＳ８４で生成した乱数Ｒ２（暗号化する前の乱数Ｒ２）と一致すれば、コンテンツプロバイダ２を適正なプロバイダとして認証し、一致しなけば、不適正なプロバイダとして、処理を終了する。

【０１１７】以上のように、EMDサービスセンタ１の相互認証部１７とコンテンツプロバイダ２の相互認証部３９は、相互認証する。相互認証に利用された乱数は、その相互認証に続く処理にだけ有効な一時鍵Ｋｔｅｍｐとして利用される。

【０１１８】図４０は、図３４のステップＳ１２および図３５のステップＳ２３に対応する、レシーバ５１がEMDサービスセンタ１のユーザ管理部１８に登録する処理を説明するフローチャートである。ステップＳ１０１において、レシーバ５１のSAM６２は、ICカードインターフェース６４の出力から、レシーバ５１にバックアップ用のICカード５５が装着されているか否かを判定し、バックアップ用のICカード５５が装着されていると判定された場合（例えば、レシーバ５１が新たなレシーバ５１に変更され、元のレシーバ５１のデータを、新たなレシーバ５１に引き継ぐために、元のレシーバ５１のデータをバックアップ用のICカード５５にバックアップさせている場合）、ステップＳ１０２に進み、ICカード５５に記憶されているバックアップデータの読み込み処理を実行する。この処理の詳細は、図４５のフローチャートを参照して後述する。勿論、この読み込み処理が実行されるためには、その前に、ICカード５５に、バックアップデータを記憶させる必要があるが、その処理は、図４３を参照して後述する。

【０１１９】ステップＳ１０１において、バックアップ用のICカード５５が装着されていないと判定された場合、手続は、ステップＳ１０２をスキップし、ステップＳ１０３に進む。ステップＳ１０３において、SAM６２の相互認証モジュール７１は、EMDサービスセンタ１の相互認証部１７と相互認証し、SAM６２は、証明書をEMDサービスセンタ１のユーザ管理部１８に送信する。この認証処理は、図３７乃至図３９を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップＳ１０３で、SAM６２がEMDサービスセンタ１のユーザ管理部１８に送信する証明書は、図４１に示すデータを含む。SAM６２が送信する証明書は、図１４に示すコンテンツプロバイダ２の証明書とほぼ同様の構成を有するが、更に、他のSAMに従属するか否かを示すデータを含んでいる。ステップＳ１０４において、SAM６２は、通信部６１を介して、一時鍵Ｋｔｅｍｐで暗号化した、ユーザの銀行等の決済機関の情報等をEMDサービスセンタ１のユーザ管理部１８に送信する。

【０１２０】ステップＳ１０５において、EMDサービスセンタ１のユーザ管理部１８は、受信したSAM６２のIDを基に、図７に示したユーザ登録データベースを検索する。ステップＳ１０６において、EMDサービスセンタ１のユーザ管理部１８は、受信したIDを有するSAM６２の登録が可能であるか否かを判定し、受信したIDを有するSAM６２の登録が可能であると判定された場合、ステップＳ１０７に進み、受信したIDを有するSAM６２が、新規登録であるか否かを判定する。ステップＳ１０７において、受信したIDを有するSAM６２が、新規登録ではないと判定された場合、手続は、ステップＳ１０８に進む。

【０１２１】ステップＳ１０８において、EMDサービスセンタ１のユーザ管理部１８は、更新登録を実行し、受信したIDを基にユーザ登録データベースを検索し、登録リストを作成する。この登録リストは、例えば、図４２に示す構造を有し、機器のSAMのIDに対応して、EMDサービスセンタ１のユーザ管理部１８が登録を拒絶したか否かを示す登録拒絶フラグ、従属する機器である場合のコンテンツ鍵Ｋｃｏの利用条件を示すステータスフラグ、従属する機器であるか否かを示すコンディションフラグ、並びに登録拒絶フラグ、ステータスフラグ、およびコンディションフラグにハッシュ関数を適用して生成したハッシュ値をEMDサービスセンタ１の秘密鍵Ｋｓｅｓｃで暗号化した署名から構成される。

【０１２２】機器のSAMのIDは、機器の固有の６４ビットからなるIDを示す（図４２では、１６進数で示す）。登録拒絶フラグの”１”は、EMDサービスセンタ１のユーザ管理部１８が対応するIDを有する機器を登録したことを示し、登録拒絶フラグの”０”は、MDサービスセンタ１のユーザ管理部１８が対応するIDを有する機器の登録を拒絶したことを示す。

【０１２３】ステータスフラグのMSB(Most Significant Bit)の”１”は、対応するIDを有する子の機器（例えばレコーダ５３）が従属した親の機器（例えばレシーバ５１）からコンテンツ鍵Ｋｃｏをもらえることを示し、ステータスフラグのMSBの”０”は、対応するIDを有する子の機器が従属した親の機器からコンテンツ鍵Ｋｃｏをもらえないことを示している。ステータスフラグの上位から２ビット目の”１”は、対応するIDを有する子の機器が従属した親の機器から、親の機器の保存用鍵Ｋｓａｖｅで暗号化されたコンテンツ鍵Ｋｃｏをもらえることを示す。ステータスフラグの上位から３ビット目の”１”は、対応するIDを有する子の機器が従属した親の機器から、配送用鍵Ｋｄで暗号化されたコンテンツ鍵Ｋｃｏをもらえることを示す。ステータスフラグのLSB(Least Significant Bit)の”１”は、従属した親の機器が配送用鍵Ｋｄで暗号化したコンテンツ鍵Ｋｃｏを購入し、対応するIDを有する子の機器に、一時鍵Ｋｔｅｍｐで暗号化してコンテンツ鍵Ｋｃｏを渡すことを示す。

【０１２４】コンディションフラグの”０”は、対応するIDを有する機器がEMDサービスセンタ１のユーザ管理部１８と直接通信が出来る（すなわち、例えばレシーバ５１のような親の機器である）ことを示し、コンディションフラグの”１”は、対応するIDを有する機器がEMDサービスセンタ１のユーザ管理部１８と直接通信が出来ない（すなわち、例えばレコーダ５３のような子の機器である）ことを示す。コンディションフラグが”０”のとき、ステータスフラグは常に”００００”に設定される。

【０１２５】ステップＳ１０９において、EMDサービスセンタ１のユーザ管理部１８は、相互認証部１７から供給された一時鍵Ｋｔｅｍｐで暗号化した、鍵サーバ１４から供給された配送用鍵Ｋｄをレシーバ５１のSAM６２に送信する。ステップＳ１１０において、レシーバ５１のSAM６２は、受信した配送用鍵Ｋｄを一時鍵Ｋｔｅｍｐで復号し、記憶モジュール７３に記憶させる。

【０１２６】ステップＳ１１１において、EMDサービスセンタ１のユーザ管理部１８は、一時鍵Ｋｔｅｍｐで暗号化した登録リストをレシーバ５１のSAM６２に送信する。ステップＳ１１２において、レシーバ５１のSAM６２は、受信した登録リストを一時鍵Ｋｔｅｍｐで復号し、記憶モジュール７３に記憶させ、処理は終了する。

【０１２７】ステップＳ１０７において、受信したIDを有するSAM６２が、新規登録であると判定された場合、手続は、ステップＳ１１４に進み、EMDサービスセンタ１のユーザ管理部１８は、新規登録を実行し、登録リストを作成し、ステップＳ１０９に進む。

【０１２８】ステップＳ１０６において、受信したIDを有するSAM６２の登録が不可であると判定された場合、ステップＳ１１３に進み、EMDサービスセンタ１のユーザ管理部１８は、登録拒絶の登録リストを作成し、ステップＳ１１１に進む。

【０１２９】このように、レシーバ５１は、EMDサービスセンタ１に登録される。

【０１３０】次に、今まで使用していたレシーバ５１の記憶モジュール７３に記憶された配送用鍵Ｋｄなどの所定のデータをICカード５５に記憶させる処理の詳細を、図４３のフローチャートを参照して説明する。ステップＳ１２１において、SAM６２の相互認証モジュール７１は、ICカード５５の相互認証モジュール８０と相互認証する。この認証処理は、図３７乃至図３９を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップＳ１２２において、SAM６２の乱数発生ユニット９２は、バックアップ鍵Ｋｉｃとして用いられる乱数を生成する。ステップＳ１２３において、SAM６２の暗号化ユニット９３は、記憶モジュール７３に記憶されているSAMのID番号、保存用鍵Ｋｓａｖｅ、およびHDD５２のIDを、バックアップ鍵Ｋｉｃを用いて暗号化する。ステップＳ１２４において、SAM６２の暗号化ユニット９３は、EMDサービスセンタ１の公開鍵Ｋｐｅｓｃでバックアップ鍵Ｋｉｃを暗号化する（SAM６２は、EMDサービスセンタ１との間の認証処理（図３９のステップＳ８９）において、EMDサービスセンタ１の公開鍵Ｋｐｅｓｃを取得している）。ステップＳ１２５において、レシーバ５１のSAM６２は、ICカードインターフェース６４を介して、暗号化されたSAMのID番号、保存用鍵Ｋｓａｖｅ、およびHDD５２のID並びに暗号化されたバックアップ鍵ＫｉｃをICカード５５に送信し、記憶モジュール８１に記憶させる。

【０１３１】以上のように、SAM６２の記憶モジュール７３に記憶されたSAMのID番号、保存用鍵Ｋｓａｖｅ、およびHDD５２のIDは、バックアップ鍵Ｋｉｃを用いて暗号化され、EMDサービスセンタ１の公開鍵Ｋｐｅｓｃを用いて暗号化されたバックアップ鍵Ｋｉｃと共に、ICカード５５の記憶モジュール８１に記憶される。

【０１３２】今まで使用していたレシーバ５１の記憶モジュール７３に記憶された配送用鍵Ｋｄなどの所定のデータをICカード５５に記憶させる他の処理の例の詳細を、図４４のフローチャートを参照して説明する。ステップＳ１３１において、SAM６２の相互認証モジュール７１は、ICカード５５の相互認証モジュール８０と相互認証する。ステップＳ１３２において、SAM６２の暗号化ユニット９３は、記憶モジュール７３に記憶されているSAMのID番号、保存用鍵Ｋｓａｖｅ、およびHDD５２の

IDを、EMDサービスセンタ１の公開鍵Ｋｐｅｓｃを用いて暗号化する。ステップＳ１３３において、レシーバ５１のSAM６２は、ICカードインターフェース６４を介して、暗号化されたSAMのID番号、保存用鍵Ｋｓａｖｅ、およびHDD５２のIDをICカード５５に送信し、記憶モジュール８１に記憶させる。

【０１３３】図４４に示す処理により、図４３に示した場合より簡単な処理で、EMDサービスセンタ１の公開鍵Ｋｐｅｓｃを用いて暗号化されたSAMのID番号、保存用鍵Ｋｓａｖｅ、およびHDD５２のIDは、ICカード５５の記憶モジュール８１に記憶される。

【０１３４】このように、ICカード５５にバックアップされたデータは、図４０のステップＳ１０２の処理で、新しいレシーバ５１に読み込まれる。図４５は、図４３に示す処理でバックアップされたデータ読み出す場合の処理を説明するフローチャートである。ステップＳ１４１において、新しいレシーバ５１のSAM６２の相互認証モジュール７１は、ICカード５５の相互認証モジュール８０と相互認証する。この認証処理は、図３７乃至図３９を参照して説明した場合と同様であるので、ここでは説明を省略する。

【０１３５】ステップＳ１４２において、SAM６２は、ICカードインタフェース６４を介して、記憶モジュール８１に記憶された、バックアップ鍵Ｋｉｃで暗号化されている古いレシーバ５１の記憶モジュール７３のデータ（SAMのID番号、保存用鍵Ｋｓａｖｅ、およびHDD５２のIDを示すバックアップデータ）、およびEMDサービスセンタ１の公開鍵Ｋｐｅｓｃで暗号化されているバックアップ鍵Ｋｉｃを読み出す。ステップＳ１４３において、SAM６２の相互認証モジュール７１は、通信部６１を介して、EMDサービスセンタ１の相互認証部１７と相互認証する。この認証処理は、図３７乃至図３９を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップＳ１４４において、SAM６２は、通信部６１を介して、バックアップ鍵Ｋｉｃで暗号化されている記憶モジュール７３のデータ、およびEMDサービスセンタ１の公開鍵Ｋｐｅｓｃで暗号化されているバックアップ鍵Ｋｉｃを、EMDサービスセンタ１のユーザ管理部１８に送信する。

【０１３６】ステップＳ１４５において、EMDサービスセンタ１のユーザ管理部１８は、受信したバックアップ鍵Ｋｉｃを自分自身の秘密鍵Ｋｓｅｓｃで復号する。ステップＳ１４６において、EMDサービスセンタ１のユーザ管理部１８は、受信したバックアップデータを、バックアップ鍵Ｋｉｃで復号する。ステップＳ１４７において、EMDサービスセンタ１のユーザ管理部１８は、復号したバックアップデータを、相互認証部１７から供給された一時鍵Ｋｔｅｍｐで、再度、暗号化する。ステップＳ１４８において、EMDサービスセンタ１のユーザ管理部１８は、一時鍵Ｋｔｅｍｐで暗号化されたバックアップデータを、レシーバ５１の通信部６１に送信する。

【０１３７】ステップＳ１４９において、レシーバ５１の通信部６１は、EMDサービスセンタ１のユーザ管理部１８から受信したデータを、SAM６２に送信し、SAM６２は、そのデータを復号した後、記憶モジュール７３に記憶させる。ステップＳ１５０において、EMDサービスセンタ１のユーザ管理部１８は、ICカード５５にデータを記憶させた古い装置のSAM６２のIDに対応するユーザ登録データベース（図７）のデータを登録不可に設定し、処理を終了する。

【０１３８】このように、新しいレシーバ５１は、ICカード５５のバックアップデータを読み込む。

【０１３９】図４４に示す処理でバックアップされたデータ読み出す場合の処理を、図４６に示すフローチャートを用いて説明する。ステップＳ１６１において、新しいレシーバ５１のSAM６２の相互認証モジュール７１は、ICカード５５の相互認証モジュール８０と相互認証する。この認証処理は、図３７乃至図３９を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップＳ１６２において、SAM６２は、ICカードインタフェース６４を介して、EMDサービスセンタ１の公開鍵Ｋｐｅｓｃで暗号化されている古いレシーバ５１の記憶モジュール７３のデータ（SAMのID番号、保存用鍵Ｋｓａｖｅ、およびHDD５２のIDを示すバックアップデータ）を読み出す。

【０１４０】ステップＳ１６３において、SAM６２の相互認証モジュール７１は、通信部６１を介して、EMDサービスセンタ１の相互認証部１７と相互認証する。この認証処理は、図３７乃至図３９を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップＳ１６４において、SAM６２は、通信部６１を介して、EMDサービスセンタ１の公開鍵Ｋｐｅｓｃで暗号化されている記憶モジュール７３のデータを、EMDサービスセンタ１のユーザ管理部１８に送信する。

【０１４１】ステップＳ１６５において、EMDサービスセンタ１のユーザ管理部１８は、受信した記憶モジュール７３のデータを自分自身の秘密鍵Ｋｓｅｓｃで復号する。ステップＳ１６６において、EMDサービスセンタ１のユーザ管理部１８は、復号したバックアップデータを、相互認証部１７から供給された一時鍵Ｋｔｅｍｐで、再度、暗号化する。ステップＳ１６７において、EMDサービスセンタ１のユーザ管理部１８は、一時鍵Ｋｔｅｍｐで暗号化されたバックアップデータを、レシーバ５１の通信部６１に送信する。

【０１４２】ステップＳ１６８において、レシーバ５１の通信部６１は、EMDサービスセンタ１のユーザ管理部１８から受信したデータを、SAM６２に送信し、SAM６２は、そにのデータを復号した後、記憶モジュール７３に記憶させる。ステップＳ１６９において、EMDサービスセンタ１のユーザ管理部１８は、ICカード５５にデータ

を記憶させた古い装置のSAM６２のIDに対応するユーザ登録データベース（図７）のデータを登録不可に設定する。

【０１４３】このように、図４４に示す処理を用いたバックアップの場合、図４６に示す処理により、新しいレシーバ５１は、ICカード５５のバックアップデータを読み込む。

【０１４４】レシーバ５１は、自分自身を登録する場合（図３４のステップＳ１２に対応する処理を実行する場合）、図４０のフローチャートに示す処理を実行するが、レシーバ５１に従属するレコーダ５３をEMDサービスセンタ１に登録する場合、図４７のフローチャートに示す処理を実行する。ステップＳ１８１において、レシーバ５１のSAM６２は、記憶モジュール７３に記憶された登録リストに、レコーダ５３のIDを書き込む。ステップＳ１８２において、レシーバ５１の相互認証モジュール７１は、EMDサービスセンタ１の相互認証部１７と相互認証する。この認証処理は、図３７乃至図３９を参照して説明した場合と同様であるので、ここでは説明を省略する。

【０１４５】ステップＳ１８３において、EMDサービスセンタ１のユーザ管理部１８は、レシーバ５１のID（図４１に示すSAM６２の証明書に含まれるSAM６２のID）を基に、ユーザ登録データベースを検索し、レシーバ５１が登録不可であるか否かを判定し、レシーバ５１が登録不可ではないと判定された場合、ステップＳ１８４に進み、レシーバ５１のSAM62は、EMDサービスセンタ１のユーザ管理部１８に、記憶モジュール７３に記憶している配送用鍵Ｋｄのバージョン、課金情報（後述の図５４に示すフローチャートのステップＳ３３７の処理で記憶される）、および登録リスト、並びにHDD５２に記録された取扱方針を一時鍵Ｋｄで暗号化し、通信部６１を介して、EMDサービスセンタ１のユーザ管理部１８に、記憶モジュール７３に記憶している配送用鍵Ｋｄのバージョン、課金情報、および登録リスト、並びにHDD５２に記録された取扱方針を送信する。ステップＳ１８５において、EMDサービスセンタ１のユーザ管理部１８は、受信したデータを復号した後、課金情報を処理し、図４２を参照して説明した、レシーバ５１から受信した登録リストのレコーダ５３に関する登録拒絶フラグ、およびステータスフラグなどのデータの部分を更新し、レシーバ５１に対応するデータに応じた署名を付する。

【０１４６】ステップＳ１８６において、EMDサービスセンタ１のユーザ管理部１８は、レシーバ５１が有する配送用鍵Ｋｄのバージョンが最新か否かを判定し、レシーバ５１が有する配送用鍵Ｋｄのバージョンが最新であると判定された場合、ステップＳ１８７に進み、一時鍵Ｋｄで暗号化した、更新した登録リスト、および課金情報受信メッセージを、レシーバ５１に送信し、レシーバ５１は、更新した登録リスト、および課金情報受信メッセージを受信し、復号した後、記憶する。ステップＳ１８８において、レシーバ５１は、記憶モジュール７３に記憶された課金情報を消去し、登録リストを、EMDサービスセンタ１のユーザ管理部１８からステップＳ１８７において受信したものに更新し、ステップＳ１９１に進む。

【０１４７】ステップＳ１８６において、レシーバ５１が有する配送用鍵Ｋｄのバージョンが最新のものではないと判定された場合、ステップＳ１８９に進み、EMDサービスセンタ１のユーザ管理部１８は、一時鍵Ｋｄで暗号化した、最新バージョンの配送用鍵Ｋｄ、更新した登録リスト、および課金情報受信メッセージを、レシーバ５１に送信し、レシーバ５１は、最新バージョンの配送用鍵Ｋｄ、更新した登録リスト、および課金情報受信メッセージを受信し、復号した後、記憶する。ステップＳ１９０において、レシーバ５１は、記憶モジュール７３に記憶された課金情報を消去し、登録リストを、EMDサービスセンタ１のユーザ管理部１８からステップＳ１８９において受信したものに更新し、配送用鍵Ｋｄを最新バージョンのものに更新し、ステップＳ１９１に進む。

【０１４８】ステップＳ１９１において、レシーバ５１のSAM６２は、更新した登録リストを参照し、レコーダ５３が登録不可か否かを判定し、レコーダ５３が登録不可でないと判定された場合、ステップＳ１９２に進み、レシーバ５１とレコーダ５３は相互認証し、一時鍵Ｋｔｅｍｐを共有する。この認証処理は、図３７乃至図３９を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップＳ１９３において、レコーダ５３に、一時鍵Ｋｄで暗号化した、登録完了メッセージ、および配送用鍵Ｋｄを送信し、レコーダ５３は、登録完了メッセージ、および配送用鍵Ｋｄを受信し、復号する。ステップＳ１９４において、レコーダ５３は、配送用鍵Ｋｄを更新し、処理は終了する。

【０１４９】ステップＳ１８３において、レシーバ５１が登録不可であると判定された場合、および、ステップＳ１９１において、レコーダ５３が登録不可であると判定された場合、処理は終了する。

【０１５０】以上のように、レシーバ５１に従属するレコーダ５３は、レシーバ５１を介して、EMDサービスセンタ１に登録される。

【０１５１】図４８は、図３４のステップＳ１３において、EMDサービスセンタ１がレシーバ５１に送信した配送用鍵Ｋｄを、レシーバ５１が受け取る処理の詳細を説明するフローチャートである。ステップＳ２０１において、レシーバ５１の相互認証モジュール７１は、EMDサービスセンタ１の相互認証部１７と相互認証する。この認証処理は、図３７乃至図３９を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップＳ２０２において、レシーバ５１のSAM６２は、通信部６１を介して、EMDサービスセンタ１のユーザ管理部１

８に証明書を送信し、EMDサービスセンタ１のユーザ管理部１８は、証明書を受信する。ステップＳ２０３乃至ステップＳ２１０は、図４７のステップＳ１８３乃至ステップＳ１９０と同様の処理であるのでその説明は省略する。

【０１５２】このように、レシーバ５１は、EMDサービスセンタ１のユーザ管理部１８から配送用鍵Ｋｄを受け取り、レシーバ５１の課金情報をEMDサービスセンタ１のユーザ管理部１８に送信する。

【０１５３】次に、レシーバ５１に従属するレコーダ５３の配送用鍵Ｋｄの受け取り処理（図４２に示すステータスフラグが、レコーダ５３の配送用鍵Ｋｄの受け取りを許可する値を有する場合）を、図４９に示すフローチャートを用いて説明する。ステップＳ２２１において、レシーバ５１の相互認証モジュール７１およびレコーダ５３の図示せぬ相互認証モジュールは、相互認証する。この認証処理は、図３７乃至図３９を参照して説明した場合と同様であるので、ここでは説明を省略する。

【０１５４】ステップＳ２２２において、レシーバ５１は、レシーバ５１の記憶モジュール７３に記憶する登録リストにレコーダ５３のデータが載っているか否かを判定し、レシーバ５１の記憶モジュール７３に記憶する登録リストにレコーダ５３のデータが載っていると判定された場合、ステップＳ２２３に進み、レシーバ５１の記憶モジュール７３に記憶する登録リストを基に、レコーダ５３が登録不可であるか否かを判定する。ステップＳ２２３において、レコーダ５３が登録不可ではないと判定された場合、ステップＳ２２４に進み、レコーダ５３のSAM６６は、レシーバ５１のSAM６２に、内蔵する記憶モジュールに記憶している配送用鍵Ｋｄ（後述する図４９のステップＳ２３５でレシーバ５１から受け取っている）のバージョンおよび課金情報（後述する図５４に対応する処理のステップＳ３３７に相当する処理で記憶している）を一時鍵Ｋｔｅｍｐで暗号化して、送信し、レシーバ５１のSAM６２は、配送用鍵Ｋｄのバージョンおよび課金情報を受信し、復号する。

【０１５５】ステップＳ２２５において、レシーバ５１の相互認証モジュール７１は、通信部６１を介して、EMDサービスセンタ１の相互認証部１７と、相互認証する。この認証処理は、図３７乃至図３９を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップＳ２２６において、EMDサービスセンタ１のユーザ管理部１８は、レシーバ５１のIDを基に、ユーザ登録データベースを検索し、レシーバ５１が登録不可であるか否かを判定し、レシーバ５１が登録不可ではないと判定された場合、ステップＳ２２７に進み、レシーバ５１のSAM62は、通信部６１を介して、EMDサービスセンタ１のユーザ管理部１８に、一時鍵Ｋｄで暗号化した、記憶モジュール７３に記憶している配送用鍵Ｋｄのバージョン、課金情報、および登録リスト、HDD５２に記録している取扱方針、並びにレコーダ５３の課金情報を送信する。ステップＳ２２８において、EMDサービスセンタ１のユーザ管理部１８は、受信したデータを復号した後、課金情報を処理し、図４２で説明した、レシーバ５１から受信した登録リストのレコーダ５３に関する登録拒絶フラグ、ステータスフラグなどのデータの部分を更新し、レシーバ５１に対応するデータに応じた署名を付する。

【０１５６】ステップＳ２２９乃至ステップＳ２３４の処理は、図４７に示すステップＳ１８６乃至ステップＳ１９１とそれぞれ同様であるので、その説明は省略する。

【０１５７】ステップＳ２３４において、レシーバ５１のSAM６２は、更新した登録リストを参照し、レコーダ５３が登録不可か否かを判定し、レコーダ５３が登録不可でないと判定された場合、ステップＳ２３５に進み、レコーダ５３に、一時鍵Ｋｄで暗号化した、課金情報受信メッセージ、および配送用鍵Ｋｄを送信し、レコーダ５３は、課金情報受信メッセージ、および配送用鍵Ｋｄを受信し、復号する。ステップＳ２３６において、レコーダ５３のSAM６６は、内蔵する記憶モジュールに記憶している、課金情報を消去し、配送用鍵Ｋｄを最新のバージョンに更新する。

【０１５８】ステップＳ２２２において、レシーバ５１の記憶モジュール７３に記憶する登録リストにレコーダ５３のデータが載っていないと判定された場合、ステップＳ２３７に進み、図４７に示したレコーダ５３の登録処理を実行し、ステップＳ２２４に進む。

【０１５９】ステップＳ２２３において、レコーダ５３が登録不可であると判定された場合、ステップＳ２２６において、レシーバ５１が登録不可であると判定された場合、および、ステップＳ２３４において、レコーダ５３が登録不可であると判定された場合、処理は終了する。

【０１６０】以上のように、レシーバ５１に従属するレコーダ５３は、レシーバ５１を介して、配送用鍵Ｋｄを受け取る。

【０１６１】次に、図３４のステップＳ１４に対応する、コンテンツプロバイダ２がサービスプロバイダ３にコンテンツプロバイダセキュアコンテナを送信する処理を、図５０のフローチャートを用いて説明する。ステップＳ２５１において、コンテンツプロバイダ２のウォータマーク付加部３２は、コンテンツサーバ３１から読み出したコンテンツに、コンテンツプロバイダ２を示す所定のウォータマークを挿入し、圧縮部３３に供給する。ステップＳ２５２において、コンテンツプロバイダ２の圧縮部３３は、ウォータマークが挿入されたコンテンツをATRAC2等の所定の方式で圧縮し、暗号化部３４に供給する。ステップＳ２５３において、乱数発生部３５は、コンテンツ鍵Ｋｃｏとして用いる乱数を発生させ、暗号

化部３４に供給する。ステップＳ２５４において、コンテンツプロバイダ２の暗号化部３４は、DESなどの所定の方式で、コンテンツ鍵Ｋｃｏを使用して、ウォータマークが挿入され、圧縮されたコンテンツを暗号化する。

【０１６２】ステップＳ２５５において、暗号化部３６は、DESなどの所定の方式で、図３４のステップＳ１１の処理により、EMDサービスセンタ１から供給されている配送用鍵Ｋｄでコンテンツ鍵Ｋｃｏを暗号化する。ステップＳ２５６において、コンテンツプロバイダ２のセキュアコンテナ作成部３８は、暗号化されたコンテンツ、暗号化されたコンテンツ鍵Ｋｃｏ、およびポリシー記憶部３７から供給された取扱方針にハッシュ関数を適用してハッシュ値を算出し、自分自身の秘密鍵Ｋｓｃｐで暗号化し、図１３に示すような署名を作成する。ステップＳ２５７において、コンテンツプロバイダ２のセキュアコンテナ作成部３８は、暗号化されたコンテンツ、暗号化されたコンテンツ鍵Ｋｃｏ、ポリシー記憶部３７から供給される取扱方針、およびステップＳ２５６で生成した署名を含んだ、図１３に示すようなコンテンツプロバイダセキュアコンテナを作成する。

【０１６３】ステップＳ２５８において、コンテンツプロバイダ２の相互認証部３９は、サービスプロバイダ３の相互認証部４５と相互認証する。この認証処理は、図３７乃至図３９を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップＳ２５９において、コンテンツプロバイダ２のセキュアコンテナ作成部３８は、サービスプロバイダ３に、コンテンツプロバイダセキュアコンテナに、予め認証局から発行してもらった証明書を付して送信し、処理を終了する。

【０１６４】以上のように、コンテンツプロバイダ２は、サービスプロバイダ３に、コンテンツプロバイダセキュアコンテナを送信する。

【０１６５】コンテンツ鍵Ｋｃｏと共に取扱方針を配送用鍵Ｋｄで暗号化する例の場合の、コンテンツプロバイダ２がサービスプロバイダ３にコンテンツプロバイダセキュアコンテナを送信する他の処理の詳細を、図５１のフローチャートを用いて説明する。ステップＳ２７１乃至ステップＳ２７４の処理は、図５０のステップＳ２５１乃至ステップＳ２５４の処理とそれぞれ同様であり、その説明は省略する。ステップＳ２７５において、コンテンツプロバイダ２の暗号化部３６は、図３５のステップＳ２１の処理により、EMDサービスセンタ１から供給されている配送用鍵Ｋｄを用いて、DESなどの所定の方式で、コンテンツ鍵Ｋｃｏおよびポリシー記憶部３７から供給される取扱方針を暗号化する。

【０１６６】ステップＳ２７６において、コンテンツプロバイダ２のセキュアコンテナ作成部３８は、暗号化されたコンテンツ、暗号化されたコンテンツ鍵Ｋｃｏ、および暗号化された取扱方針にハッシュ関数を適用しハッシュ値を算出し、自分自身の秘密鍵Ｋｓｃｐで暗号化し、図２５に示すような署名を作成する。ステップＳ２７７において、コンテンツプロバイダ２のセキュアコンテナ作成部３８は、暗号化されたコンテンツ、暗号化されたコンテンツ鍵Ｋｃｏ、暗号化された取扱方針、および署名を含んだ、図２５に示すようなコンテンツプロバイダセキュアコンテナを作成する。ステップＳ２７８およびステップＳ２７９の処理は、図５０のステップＳ２５８およびステップＳ２５９の処理とそれぞれ同様であり、その説明は省略する。

【０１６７】このように、コンテンツプロバイダ２は、サービスプロバイダ３に、暗号化された取扱方針を含むコンテンツプロバイダセキュアコンテナを送信する。

【０１６８】次に、図３４のステップＳ１５に対応する、サービスプロバイダ３がレシーバ５１にサービスプロバイダセキュアコンテナを送信する処理の詳細を図５２のフローチャートを用いて説明する。ステップＳ２９１において、サービスプロバイダ３の値付け部４２は、コンテンツプロバイダ２のセキュアコンテナ作成部３８から送信されたコンテンツプロバイダセキュアコンテナに付された証明書に含まれる署名を確認し、証明書の改竄がなければ、コンテンツプロバイダ２の公開鍵Ｋｐｃｐを取り出す。証明書の署名の確認は、図３９のステップＳ８３における処理と同様であるので、その説明は省略する。

【０１６９】ステップＳ２９２において、サービスプロバイダ３の値付け部４２は、コンテンツプロバイダ２のセキュアコンテナ作成部３８から送信されたコンテンツプロバイダセキュアコンテナの署名をコンテンツプロバイダ２の公開鍵Ｋｐｃｐで復号し、得られたハッシュ値が、暗号化されたコンテンツ、暗号化されたコンテンツ鍵Ｋｃｏ、および取扱方針にハッシュ関数を適用し得られたハッシュ値と一致することを確認し、コンテンツプロバイダセキュアコンテナの改竄がないことを確認する。改竄が発見された場合は、処理を終了する。

【０１７０】コンテンツプロバイダセキュアコンテナに改竄がない場合、ステップＳ２９３において、サービスプロバイダ３の値付け部４２は、コンテンツプロバイダセキュアコンテナから取扱方針を取り出す。ステップＳ２９４において、サービスプロバイダ３の値付け部４２は、取扱方針を基に、図１７で説明した価格情報を作成する。ステップＳ２９５において、サービスプロバイダ３のセキュアコンテナ作成部４４は、暗号化されたコンテンツ、暗号化されたコンテンツ鍵Ｋｃｏ、取扱方針、価格情報、並びに暗号化されたコンテンツ、暗号化されたコンテンツ鍵Ｋｃｏ、取扱方針、および価格情報にハッシュ関数を適用して得られたハッシュ値を、自分自身の秘密鍵Ｋｓｓｐで暗号化し、得られた値を署名として図１５に示すようなサービスプロバイダセキュアコンテナを作成する。

【０１７１】ステップＳ２９６において、サービスプロ

バイダ３の相互認証部４５は、レシーバ５１の相互認証モジュール７１と相互認証する。この認証処理は、図３７乃至図３９を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップＳ２９７において、サービスプロバイダ３のセキュアコンテナ作成部４４は、レシーバ５１の通信部６１に、証明書を付したサービスプロバイダセキュアコンテナを送信し、処理を終了する。

【０１７２】このように、サービスプロバイダ３は、レシーバ５１にサービスプロバイダセキュアコンテナを送信する。

【０１７３】コンテンツプロバイダ２において、取扱方針が配送用鍵Ｋｄで暗号化され、かつ、サービスプロバイダ３が取扱制御情報を作成する例の場合の、サービスプロバイダ３がレシーバ５１にサービスプロバイダセキュアコンテナを送信する処理の詳細を、図５３のフローチャートを用いて説明する。ステップＳ３１１およびステップＳ３１２の処理は、図５２のステップＳ２９１およびステップＳ２９２の処理とそれぞれ同様であるので、その説明は省略する。ステップＳ３１３において、サービスプロバイダ３の値付け部４２は、コンテンツプロバイダセキュアコンテナに含まれる暗号化された取扱方針を復号する。ステップＳ３１４において、サービスプロバイダ３の値付け部４２は、取扱方針を基に、図２３で説明した取扱制御情報を作成する。ステップＳ３１５乃至ステップＳ３１８の処理は、図５２のステップＳ２９４およびステップＳ２９７の処理とそれぞれ同様であるので、その説明は省略する。

【０１７４】このように、サービスプロバイダ３は、レシーバ５１に暗号化された取扱方針を含むサービスプロバイダセキュアコンテナを送信する。

【０１７５】図３４のステップＳ１６に対応する、適正なサービスプロバイダセキュアコンテナを受信した後の、レシーバ５１の課金処理の詳細を、図５４のフローチャートを用いて説明する。ステップＳ３３１において、レシーバ５１の復号／暗号化モジュール７４は、配送用鍵Ｋｄでコンテンツ鍵Ｋｃｏを復号できるか否かを判定し、配送用鍵Ｋｄでコンテンツ鍵Ｋｃｏを復号できないと判定された場合、ステップＳ３３２で、レシーバ５１は、図４８で説明した配送用鍵Ｋｄの受け取り処理を実行し、ステップＳ３３３に進む。ステップＳ３３１において、配送用鍵Ｋｄでコンテンツ鍵Ｋｃｏを復号できると判定された場合、手続は、ステップＳ３３２をスキップし、ステップＳ３３３に進む。ステップＳ３３３において、レシーバ５１の復号ユニット９１は、図３４のステップＳ１３の処理により、記憶モジュール７３に記憶されている配送用鍵Ｋｄで、コンテンツ鍵Ｋｃｏを復号する。

【０１７６】ステップＳ３３４において、レシーバ５１の課金処理モジュール７２は、サービスプロバイダセキュアコンテナに含まれる取扱方針および価格情報を取り出し、図１９および図２０で説明した課金情報および使用許諾条件情報を生成する。ステップＳ３３５において、レシーバ５１の課金処理モジュール７２は、記憶モジュール７３に記憶している課金情報およびステップＳ３３４で算出された課金情報から、現在の課金が課金の上限以上であるか否かを判定し、現在の課金が課金の上限以上であると判定された場合、ステップＳ３３６に進み、レシーバ５１は図４８で説明した配送用鍵Ｋｄの受け取り処理を実行し、新たな配送用鍵Ｋｄを受け取り、ステップＳ３３７に進む。ステップＳ３３５において、現在の課金が課金の上限未満であると判定された場合、ステップＳ３３６はスキップされ、ステップＳ３３７に進む。

【０１７７】ステップＳ３３７において、レシーバ５１の課金処理モジュール７２は、記憶モジュール７３に課金情報を記憶させる。ステップＳ３３８において、レシーバ５１の課金処理モジュール７２は、ステップＳ３３４にて生成した使用許諾条件情報をHDD５２に記録する。ステップＳ３３９において、レシーバ５１のSAM６２は、HDD５２にサービスプロバイダセキュアコンテナから取り出した取扱方針を記録させる。

【０１７８】ステップＳ３４０において、レシーバ５１の復号／暗号化モジュール７４は、使用許諾条件情報にハッシュ関数を適用しハッシュ値を算出する。ステップＳ３４１において、レシーバ５１の記憶モジュール７３は、使用許諾条件情報のハッシュ値を記憶する。記憶モジュール７３に保存用鍵Ｋｓａｖｅが記憶されていない場合、ステップＳ３４２において、レシーバ５１の乱数発生ユニット９２は、保存用鍵Ｋｓａｖｅである乱数を発生し、ステップＳ３４３に進む。記憶モジュール７３に保存用鍵Ｋｓａｖｅが記憶されている場合、ステップＳ３４２はスキップされ、ステップＳ３４３に進む。

【０１７９】ステップＳ３４３において、レシーバ５１の暗号化ユニット９３は、コンテンツ鍵Ｋｃｏを保存用鍵Ｋｓａｖｅで暗号化する。ステップＳ３４４において、レシーバ５１のSAM６２は、暗号化されたコンテンツ鍵ＫｃｏをHDD５２に記憶させる。記憶モジュール７３に保存用鍵Ｋｓａｖｅが記憶されていない場合、ステップＳ３４５において、レシーバ５１の復号／暗号化モジュール７４は、保存用鍵Ｋｓａｖｅを記憶モジュール７３に記憶させ、処理は終了する。記憶モジュール７３に保存用鍵Ｋｓａｖｅが記憶されている場合、ステップＳ３４５はスキップされ、処理は終了する。

【０１８０】以上のように、レシーバ５１は、課金情報を記憶モジュール７３に記憶すると共に、コンテンツ鍵Ｋｃｏを配送用鍵Ｋｄで復号し、再度、コンテンツ鍵Ｋｃｏを保存用鍵Ｋｓａｖｅで暗号化し、HDD５２に記録させる。保存用鍵Ｋｓａｖｅは、記憶モジュール７３に記憶される。

【０１８１】レコーダ５３も、同様の処理で、課金情報をSAM６６内の記憶モジュールに記憶すると共に、コンテンツ鍵Ｋｃｏを配送用鍵Ｋｄで復号し、再度、コンテンツ鍵Ｋｃｏを保存用鍵Ｋｓａｖｅで暗号化し、HDD５２に記録させる。保存用鍵Ｋｓａｖｅは、SAM６６内の記憶モジュールに記憶される。

【０１８２】図３４のステップＳ１７に対応するレシーバ５１がコンテンツを再生する処理の詳細を、図５５のフローチャートを用いて説明する。ステップＳ３６１において、レシーバ５１の復号／暗号化モジュール７４は、HDD５２から、図５４のステップＳ３３８で記憶した使用許諾条件情報およびステップＳ３４４で記憶した暗号化されたコンテンツ鍵Ｋｃｏを読み出す。ステップＳ３６２において、レシーバ５１の復号／暗号化モジュール７４は、使用許諾条件情報にハッシュ関数を適用しハッシュ値を算出する。

【０１８３】ステップＳ３６３において、レシーバ５１の復号／暗号化モジュール７４は、ステップＳ３６２において算出されたハッシュ値が、図５４のステップＳ３４０で記憶モジュール７３に記憶されたハッシュ値と一致するか否かを判定し、ステップＳ３６２において算出されたハッシュ値が、記憶モジュール７３に記憶されたハッシュ値と一致すると判定された場合、ステップＳ３６４に進み、使用回数の値などの使用許諾条件情報に含まれる所定の情報を更新する。ステップＳ３６５において、レシーバ５１の復号／暗号化モジュール７４は、更新した使用許諾条件情報にハッシュ関数を適用しハッシュ値を算出する。ステップＳ３６６において、レシーバ５１の記憶モジュール７３は、ステップＳ３６５で算出した使用許諾条件情報のハッシュ値を記憶する。ステップＳ３６７において、レシーバ５１の復号／暗号化モジュール７４は、HDD５２に更新した使用許諾条件情報を記録させる。

【０１８４】ステップＳ３６８において、SAM６２の相互認証モジュール７１と伸張部６３の相互認証モジュール７５は、相互認証し、SAM６２および伸張部６３は、一時鍵Ｋｔｅｍｐを記憶する。この認証処理は、図３７乃至図３９を参照して説明した場合と同様であるので、ここでは説明を省略する。相互認証に用いられる乱数Ｒ１、Ｒ２、またはＲ３が、一時鍵Ｋｔｅｍｐとして用いられる。ステップＳ３６９において、復号／暗号化モジュール７４の復号ユニット９１は、図５４のステップＳ３４４にてHDD５２に記録されたコンテンツ鍵Ｋｃｏを、記憶モジュール７３に記憶された保存用鍵Ｋｓａｖｅで復号する。ステップＳ３７０において、復号／暗号化モジュール７４の暗号化ユニット９３は、復号されたコンテンツ鍵Ｋｃｏを一時鍵Ｋｔｅｍｐで暗号化する。ステップＳ３７１において、SAM６２は、一時鍵Ｋｔｅｍｐで暗号化されたコンテンツ鍵Ｋｃｏを伸張部６３に送信する。

【０１８５】ステップＳ３７２において、伸張部６３の復号モジュール７６は、コンテンツ鍵Ｋｃｏを一時鍵Ｋｔｅｍｐで復号する。ステップＳ３７３において、SAM６２は、HDD５２に記録されたコンテンツを読み出し、伸張部６３に送信する。ステップＳ３７４において、伸張部６３の復号モジュール７７は、コンテンツをコンテンツ鍵Ｋｃｏで復号する。ステップＳ３７５において、伸張部６３の伸張モジュール７８は、復号されたコンテンツをATRAC2などの所定の方式で伸張する。ステップＳ３７６において、伸張部６３のウォータマーク付加モジュール７９は、伸張されたコンテンツにレシーバ５１を特定する所定のウォータマークを挿入する。ステップＳ３７７において、レシーバ５１は、図示せぬスピーカなどに再生されたコンテンツを出力し、処理を終了する。

【０１８６】ステップＳ３６３において、ステップＳ３６２において算出されたハッシュ値が、記憶モジュール７３に記憶されたハッシュ値と一致しないと判定された場合、ステップＳ３７８において、SAM６２は、図示せぬ表示装置にエラーメッセージを表示させる等の所定のエラー処理を実行し、処理は終了する。

【０１８７】このように、レシーバ５１は、コンテンツを再生する。

【０１８８】図５６は、図１１の構成を有するユーザホームネットワーク５において、レシーバ５１がデコーダ５６にコンテンツを再生させる処理を説明するフローチャートである。ステップＳ３９１乃至ステップＳ３９７の処理は、図５５のステップＳ３６１乃至ステップＳ３６７の処理とそれぞれ同様であるので、その説明は省略する。

【０１８９】ステップＳ３９８において、SAM６２の相互認証モジュール７１とデコーダ５６の相互認証モジュール１０１は、相互認証し、一時鍵Ｋｔｅｍｐが共有される。この認証処理は、図３７乃至図３９を参照して説明した場合と同様であるので、ここでは説明を省略する。相互認証に用いられる乱数Ｒ１、Ｒ２、またはＲ３が、一時鍵Ｋｔｅｍｐとして用いられる。ステップＳ３９９において、復号／暗号化モジュール７４の復号ユニット９１は、HDD５２に記録されたコンテンツ鍵Ｋｃｏを、記憶モジュール７３に記憶された保存用鍵Ｋｓａｖｅで復号する。ステップＳ４００において、復号／暗号化モジュール７４の暗号化ユニット９３は、復号されたコンテンツ鍵Ｋｃｏを一時鍵Ｋｔｅｍｐで暗号化する。ステップＳ４０１において、SAM６２は、一時鍵Ｋｔｅｍｐで暗号化されたコンテンツ鍵Ｋｃｏをデコーダ５６に送信する。

【０１９０】ステップＳ４０２において、デコーダ５６の復号モジュール１０２は、コンテンツ鍵Ｋｃｏを一時鍵Ｋｔｅｍｐで復号する。ステップＳ４０３において、SAM６２は、HDD５２に記録されたコンテンツを読み出し、デコーダ５６に送信する。ステップＳ４０４におい

て、デコーダ５６の復号モジュール１０３は、コンテンツをコンテンツ鍵Ｋｃｏで復号する。ステップＳ４０５において、デコーダ５６の伸張モジュール１０４は、復号されたコンテンツをATRAC2などの所定の方式で伸張する。ステップＳ４０６において、デコーダ５６のウォータマーク付加モジュール１０５は、伸張されたコンテンツにデコーダ５６を特定する所定のウォータマークを挿入する。ステップＳ４０７において、デコーダ５６は、図示せぬスピーカなどに再生されたコンテンツを出力し、処理を終了する。

【０１９１】ステップＳ４０８の処理は、図５５のステップＳ３７８の処理と同様であるので、その説明は省略する。

【０１９２】以上のように、ユーザホームネットワークが図１１に示す構成を有する場合、レシーバ５１が受信したコンテンツは、デコーダ５６で再生される。

【０１９３】図６１を参照して後述する決済処理の前に行われる、EMDサービスセンタ１の決済オブジェクトを作成する処理を、図５７のフローチャートを参照して説明する。ステップＳ４２１において、EMDサービスセンタ１の経歴データ管理部１５は、図４７のステップＳ１８７またはステップＳ１８９などでユーザホームネットワーク５から受信し、記憶した課金情報の中から、所定のコンテンツの利用に関する課金情報を選択し、選択した課金情報を利益分配部１６に送信する。ステップＳ４２２において、利益分配部１６は、経歴データ管理部１５から受信した課金情報にコンテンツプロバイダ２およびサービスプロバイダ３への利益配分を示すデータが含まれているか否かを判定し、経歴データ管理部１５から受信した課金情報にコンテンツプロバイダ２およびサービスプロバイダ３への利益配分を示すデータが含まれていると判定された場合、ステップＳ４２３に進む。

【０１９４】ステップＳ４２３において、利益分配部１６は、課金情報に含まれる利益配分を示すデータを参照して、所定のコンテンツを利用したユーザからサービスプロバイダ３への支払い額を算出する。ステップＳ４２４において、利益分配部１６は、課金情報に含まれる利益配分を示すデータを参照して、サービスプロバイダ３からコンテンツプロバイダ２への支払い額を算出する。ステップＳ４２５において、利益分配部１６は、課金情報に含まれる利益配分を示すデータを参照して、コンテンツプロバイダ２から権利団体への支払い額を算出し、ステップＳ４２９に進む。

【０１９５】ステップＳ４２２において、経歴データ管理部１５から受信した課金情報にコンテンツプロバイダ２およびサービスプロバイダ３への利益配分を示すデータが含まれていないと判定された場合、ステップＳ４２６に進み、利益分配部１６は、利益分配部１６が記憶する利益配分データベースを参照して、所定のコンテンツを利用したユーザからサービスプロバイダ３への支払い額を算出する。ステップＳ４２７において、利益分配部１６は、利益分配部１６が記憶する利益配分データベースを参照して、サービスプロバイダ３からコンテンツプロバイダ２への支払い額を算出する。ステップＳ４２８において、利益分配部１６は、利益分配部１６が記憶する利益配分データベースを参照して、コンテンツプロバイダ２から権利団体への支払い額を算出し、ステップＳ４２９に進む。

【０１９６】ステップＳ４２９において、利益分配部１６は、利益分配部１６に記憶されている割引情報データベースのデータを参照して、所定のユーザからサービスプロバイダ３への支払い額、サービスプロバイダ３からコンテンツプロバイダ２への支払い額、およびコンテンツプロバイダ２から権利団体への支払額を補正する。

【０１９７】ステップＳ４３０において、経歴データ管理部１５は、すべてのコンテンツについてステップＳ４２３乃至ステップＳ４２９の計算を実行したか否かを判定し、すべてのコンテンツについてステップＳ４２３乃至ステップＳ４２９の計算をまだ実行していないと判定された場合、手続きは、ステップＳ４２１に戻り、それ以降の処理を繰り返す。ステップＳ４３０において、すべてのコンテンツについてステップＳ４２１乃至ステップＳ４２９の計算が実行されたと判定された場合、手続きは、ステップＳ４３１に進む。

【０１９８】ステップＳ４３１において、利益分配部１６は、ユーザ毎に各サービスプロバイダ３への支払金額を算出し、クレジット決済オブジェクト１（例えば、ユーザがクレジットカードを使用して利用料金を支払う場合、図５８（Ａ）に示すクレジット決済オブジェクト１）を作成する。クレジット決済オブジェクト１では、支払元にユーザのIDが設定され、支払先にサービスプロバイダ３のIDが設定され、支払額にサービスプロバイダ３への支払額が設定される。ステップＳ４３２において、利益分配部１６は、サービスプロバイダ３毎に各コンテンツプロバイダ２への支払金額を算出し、クレジット決済オブジェクト２（例えば、ユーザがクレジットカードを使用して利用料金を支払う場合、図５８（Ｂ）に示すクレジット決済オブジェクト２）を作成する。クレジット決済オブジェクト２では、支払元にクレジット決済オブジェクト１が設定され、支払先にコンテンツプロバイダ２のIDが設定され、支払額にコンテンツプロバイダ２への支払額が設定される。

【０１９９】ステップＳ４３３において、利益分配部１６は、コンテンツプロバイダ２毎に権利団体への支払金額を算出し、クレジット決済オブジェクト３（例えば、ユーザがクレジットカードを使用して利用料金を支払う場合、図５８（Ｃ）に示すクレジット決済オブジェクト３）を作成する。クレジット決済オブジェクト３では、支払元にクレジット決済オブジェクト１が設定され、支払先に権利団体のIDが設定され、支払額に権利団体への

45

支払額が設定される。ステップＳ４３４において、課金請求部１９は、課金請求部１９が記憶する、ユーザに対するEMDサービスセンタ１の利用料金を格納するユーザ利用料金テーブルを参照してユーザからの徴収金額を算出し、クレジット決済オブジェクト４（例えば、ユーザがクレジットカードを使用して利用料金を支払う場合、図５８（Ｄ）に示すクレジット決済オブジェクト４）を作成し、クレジット決済オブジェクト１の徴収額を設定し、処理を終了する。クレジット決済オブジェクト４では、支払元にクレジット決済オブジェクト１が設定され、支払先にEMDサービスセンタ１のIDが設定され、支払額にEMDサービスセンタ１への支払額が設定される。

【０２００】以上のように、EMDサービスセンタ１は、決済オブジェクトを作成する。

【０２０１】図５９は、サービスプロバイダ３、コンテンツプロバイダ２、および権利団体が、EMDサービスセンタ１にサービス料を銀行決済で支払う場合の、銀行決済オブジェクトの例を示す図である。図５９（Ａ）の銀行決済オブジェクト１では、支払元にサービスプロバイダ３のIDが設定され、徴収額にサービスプロバイダ３からの徴収額が設定され、支払先にEMDサービスセンタ１のIDが設定され、支払額にEMDサービスセンタ１への支払額（徴収額と同額）が設定される。図５９（Ｂ）の銀行決済オブジェクト２では、支払元にコンテンツプロバイダ２のIDが設定され、徴収額にコンテンツプロバイダ２からの徴収額が設定され、支払先にEMDサービスセンタ１のIDが設定され、支払額にEMDサービスセンタ１への支払額（徴収額と同額）が設定される。図５９（Ｃ）の銀行決済オブジェクト３では、支払元に権利団体のIDが設定され、徴収額に権利団体からの徴収額が設定され、支払先にEMDサービスセンタ１のIDが設定され、支払額にEMDサービスセンタ１への支払額（徴収額と同額）が設定される。

【０２０２】図６０は、ユーザがクレジットカードを利用して料金を支払い、サービスプロバイダ３、およびコンテンツプロバイダ２は銀行口座を利用して決済を行う場合の、決済オブジェクトの例を示す図である。図６０（Ａ）および図６０（Ｄ）のクレジット決済オブジェクトは、図５８（Ａ）および図５８（Ｄ）のクレジット決済オブジェクトとそれぞれ同様であり、その説明は省略する。図６０（Ｂ）の銀行決済オブジェクト２は、支払元にサービスプロバイダ３のIDが設定され、徴収額に、コンテンツプロバイダ２への支払額と権利団体への支払額を合わせた、サービスプロバイダ３からの金額が設定され、支払先にコンテンツプロバイダ２のIDが設定され、支払額にコンテンツプロバイダ２への支払額（徴収額と同額）が設定される。図６０（Ｃ）の銀行決済オブジェクト３は、支払元にコンテンツプロバイダ２のIDが設定され、徴収額に、コンテンツプロバイダ２からの徴収額が設定され、支払先に権利団体のIDが設定され、支払額に権利団体への支払額（徴収額と同額）が設定される。

46

【０２０３】図５８、図５９、および図６０の決済オブジェクトに記述された、支払先、徴収額、支払先、および支払額に基づき、決済が実行されことにより、EMDサービスセンタ１、コンテンツプロバイダ２、サービスプロバイダ３、および権利団体に所定の金額が支払われる。EMDサービスセンタ１のクレジット決済処理オブジェクトを用いる決済の処理を図６１のフローチャートを参照して説明する。ステップＳ４５１において、EMDサービスセンタ１の出納部２０は、クレジット決済オブジェクトの支払先に記載されているIDより、支払先の銀行などの決済機関を求める。ステップＳ４５２において、EMDサービスセンタ１の出納部２０は、クレジット決済オブジェクトの支払元に記載されているIDより、支払元のクレジット会社などの決済機関を求める。ステップＳ４５３において、出納部２０は、予め記憶された情報により、支払元の与信処理が必要であるか否かを判定し、支払元の与信処理が必要であると判定された場合、ステップＳ４５４において、与信処理を実行する。ステップＳ４５４の与信処理において、支払元が支払いできないと判定された場合、処理は終了する。ステップＳ４５４の与信処理において、支払元が支払いできると判定された場合、ステップＳ４５５に進む。

【０２０４】ステップＳ４５３において、支払元の与信処理が必要でないと判定された場合、手続きは、ステップＳ４５４をスキップし、ステップＳ４５５に進む。

【０２０５】ステップＳ４５５において、出納部２０は、前に実行された決済オブジェクトの処理が完了しているか否かを判定し、前に実行された決済オブジェクトの処理が完了していると判定された場合、ステップＳ４５６に進み、ステップＳ４５１およびステップＳ４５２で求めた決済機関に、クレジット決済オブジェクトに記載された徴収額、および支払い額に対応した決済命令を送信する。ステップＳ４５７において、クレジット決済オブジェクトの支払先に記載されているIDに対応する支払い先にステップＳ４５６で実行した決済処理の情報を送信する。ステップＳ４５８において、クレジット決済オブジェクトの支払元に記載されているIDに対応する支払い元にステップＳ４５６で実行した決済処理の情報を送信し、処理は終了する。

【０２０６】ステップＳ４５５において、前に実行された決済オブジェクトの処理が完了していないと判定された場合、ステップＳ４５９に進み、出納部２０は、処理が完了していない決済オブジェクトに記載された支払い元に所定のメッセージを送信する等の、決済未完了の所定のエラー処理を実行し、処理は終了する。

【０２０７】以上のように、クレジット決済処理オブジェクトを用いる決済が処理される。

【０２０８】図６２は、EMDサービスセンタ１の銀行決

済処理オブジェクトを用いる決済の処理を説明するフローチャートである。銀行決済処理オブジェクトを用いる決済の処理は、図６１に示すクレジット決済処理オブジェクトを用いる決済の処理から、ステップＳ４５１およびステップＳ４５４の与信に関する処理を除いたものと同様である。ステップＳ４７１およびステップＳ４７２の処理は、図６１のステップＳ４５１およびステップＳ４５２の処理とそれぞれ同様であるので、その説明は省略する。ステップＳ４７３乃至ステップＳ４７７の処理は、図６１のステップＳ４５５乃至ステップＳ４５９の処理とそれぞれ同様であるので、その説明は省略する。

【０２０９】このように、銀行決済処理オブジェクトを用いる決済が処理され、クレジット決済処理オブジェクトを用いる決済の処理とともに、ユーザ、コンテンツプロバイダ２、サービスプロバイダ３、および権利団体から所定の金額が徴収され、EMDサービスセンタ１、コンテンツプロバイダ２、サービスプロバイダ３、および権利団体に所定の金額が入金される。

【０２１０】なお、コンテンツは、音楽データを例に説明したが、音楽データに限らず、動画像データ、静止画像データ、文書データ、またはプログラムデータでもよい。その際、圧縮は、コンテンツの種類に適した方式、例えば、画像であればMPEG(Moving Picture Experts Group)などが利用される。ウォーターマークも、コンテンツの種類に適した形式のウォーターマークが利用される。

【０２１１】また、共通鍵暗号は、ブロック暗号であるDESを使用して説明したが、NTT（商標）が提案するFEAL、IDEA(International Data Encription Algorithm)、または１ビット乃至数ビット単位で暗号化するストリーム暗号などでもよい。

【０２１２】さらに、コンテンツおよびコンテンツ鍵Ｋｃｏの暗号化は、共通鍵暗号方式を利用するとして説明したが、公開鍵暗号方式でもよい。

【０２１３】なお、本明細書において、システムとは、複数の装置により構成される装置全体を表すものとする。

【０２１４】また、上記したような処理を行うコンピュータプログラムをユーザに提供する提供媒体としては、磁気ディスク、CD-ROM、固体メモリなどの記録媒体の他、ネットワーク、衛星などの通信媒体を利用することができる。

【０２１５】

【発明の効果】請求項１に記載の情報処理装置、請求項６に記載の情報処理方法、および請求項７に記載の提供媒体によれば、情報を特定するデータおよび情報の利用に対する情報提供業者の支払い金額を示すデータを記憶し、記憶するデータを基に、情報提供業者毎の支払い金額の合計を算出し、情報提供業者毎の利益を基に、決済機関に対し情報提供業者毎の決済を指示するようにしたので、精算処理および利益の算出の処理が効率良く出来るようになる。

【図面の簡単な説明】

【図１】EMDのシステムを説明する図である。

【図２】EMDサービスセンタ１の機能の構成を示すブロック図である。

【図３】EMDサービスセンタ１の配送用鍵Ｋｄの送信を説明する図である。

【図４】EMDサービスセンタ１の配送用鍵Ｋｄの送信を説明する図である。

【図５】EMDサービスセンタ１の配送用鍵Ｋｄの送信を説明する図である。

【図６】EMDサービスセンタ１の配送用鍵Ｋｄの送信を説明する図である。

【図７】ユーザ登録データベースを説明する図である。

【図８】コンテンツプロバイダ２の機能の構成を示すブロック図である。

【図９】サービスプロバイダ３の機能の構成を示すブロック図である。

【図１０】ユーザホームネットワーク５の構成を示すブロック図である。

【図１１】ユーザホームネットワーク５の構成を示すブロック図である。

【図１２】コンテンツおよびコンテンツに付随する情報を説明する図である。

【図１３】コンテンツプロバイダセキュアコンテナを説明する図である。

【図１４】コンテンツプロバイダ２の証明書を説明する図である。

【図１５】サービスプロバイダセキュアコンテナを説明する図である。

【図１６】サービスプロバイダ３の証明書を説明する図である。

【図１７】取扱方針、価格情報、および使用許諾条件情報を示す図である。

【図１８】シングルコピーおよびマルチコピーを説明する図である。

【図１９】取扱方針および価格情報を説明する図である。

【図２０】取扱方針、価格情報、および使用許諾条件情報を説明する図である。

【図２１】コンテンツおよびコンテンツに付随する情報の他の構成を説明する図である。

【図２２】サービスプロバイダセキュアコンテナを説明する図である。

【図２３】取扱方針、取扱制御情報、価格情報、及び使用許諾条件の構成を示す図である。

【図２４】コンテンツおよびコンテンツに付随する情報の他の構成を説明する図である。

【図２５】コンテンツプロバイダセキュアコンテナを説

明する図である。

【図２６】サービスプロバイダセキュアコンテナを説明する図である。

【図２７】EMDサービスセンタ１が、決算処理に必要なデータを収集する動作を説明する図である。

【図２８】利益配分データベースの例を示す図である。

【図２９】割引テーブルの例を示す図である。

【図３０】ユーザ利用料金テーブルの例を示す図である。

【図３１】EMDサービスセンタ１の、ユーザホームネットワーク５からの課金情報の受信のときの動作を説明する図である。

【図３２】EMDサービスセンタ１の利益分配処理の動作を説明する図である。

【図３３】EMDサービスセンタ１の、コンテンツの利用実績の情報をJASRACに送信する処理の動作を説明する図である。

【図３４】コンテンツの配布の処理を説明するフローチャートである。

【図３５】コンテンツの配布の処理を説明するフローチャートである。

【図３６】EMDサービスセンタ１がコンテンツプロバイダ２へ配送用鍵Ｋｄを送信する処理を説明するフローチャートである。

【図３７】コンテンツプロバイダ２とEMDサービスセンタ１との相互認証の動作を説明するフローチャートである。

【図３８】コンテンツプロバイダ２とEMDサービスセンタ１との相互認証の動作を説明するフローチャートである。

【図３９】コンテンツプロバイダ２とEMDサービスセンタ１との相互認証の動作を説明するフローチャートである。

【図４０】レシーバ５１のEMDサービスセンタ１への登録の処理を説明するフローチャートである。

【図４１】SAMの証明書を説明する図である。

【図４２】登録リストを説明する図である。

【図４３】ICカード５５へのSAM６２のデータのバックアップの処理を説明するフローチャートである。

【図４４】ICカード５５へのSAM６２のデータのバックアップの処理を説明するフローチャートである。

【図４５】新しいレシーバにICカード５５のバックアップデータを読み込ませる処理を説明するフローチャートである。

【図４６】新しいレシーバにICカード５５のバックアップデータを読み込ませる処理を説明するフローチャートである。

【図４７】レシーバ５１が、従属関係のあるレコーダ５３をEMDサービスセンタ１に登録する処理を説明するフローチャートである。

【図４８】レシーバ５１がEMDサービスセンタ１から配送用鍵Ｋｄを受け取る処理を説明するフローチャートである。

【図４９】レコーダの配送用鍵Ｋｄの受け取り処理を説明するフローチャートである。

【図５０】コンテンツプロバイダ２がサービスプロバイダ３にコンテンツプロバイダセキュアコンテナを送信する処理を説明するフローチャートである。

【図５１】コンテンツプロバイダ２がサービスプロバイダ３にコンテンツプロバイダセキュアコンテナを送信する他の処理を説明するフローチャートである。

【図５２】サービスプロバイダ３がレシーバ５１にサービスプロバイダセキュアコンテナを送信する処理を説明するフローチャートである。

【図５３】サービスプロバイダ３がレシーバ５１にサービスプロバイダセキュアコンテナを送信する処理を説明するフローチャートである。

【図５４】レシーバ５１の課金処理を説明するフローチャートである。

【図５５】レシーバ５１がコンテンツを再生する処理を説明するフローチャートである。

【図５６】レシーバ５１がデコーダ５６にコンテンツを再生させる処理を説明するフローチャートである。

【図５７】EMDサービスセンタ１の決済オブジェクトを作成する処理を説明するフローチャートである。

【図５８】クレジット決済オブジェクトの例を説明する図である。

【図５９】銀行決済オブジェクトの例を説明する図である。

【図６０】クレジット決済オブジェクトの例および銀行決済オブジェクトの例を説明する図である。

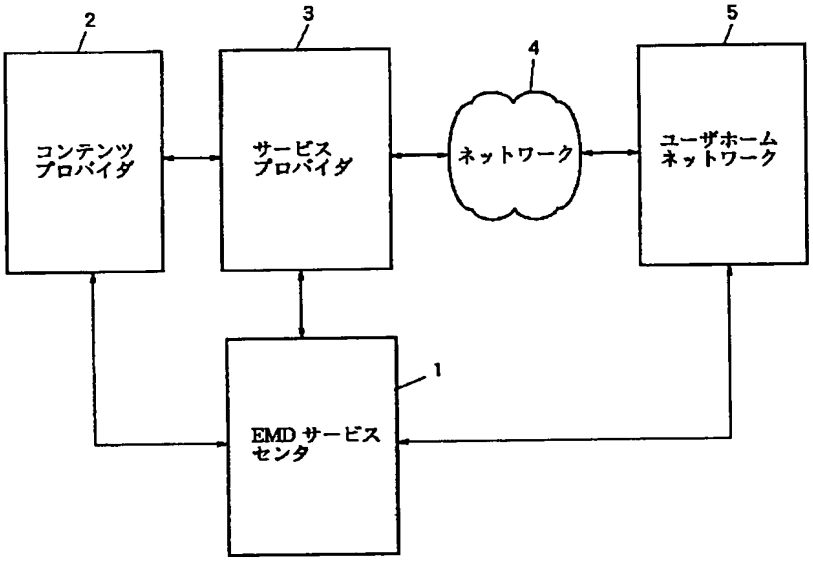
【図６１】クレジット決済処理を説明するフローチャートである。

【図６２】銀行決済処理を説明するフローチャートである。

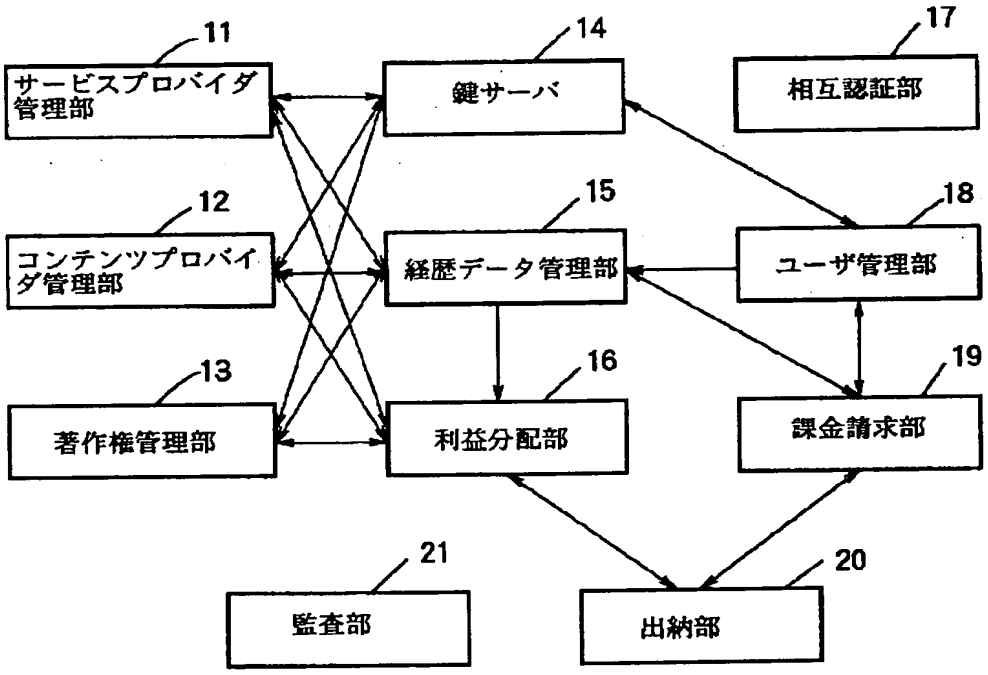
【符号の説明】

１　EMDサービスセンタ，　２　コンテンツプロバイダ，　３　サービスプロバイダ，５　ユーザホームネットワーク，　１５　経歴データ管理部，　１６利益分配部，　１８　ユーザ管理部，　２０　出納部，　４２　値付け部，　５１　レシーバ，　５６　デコーダ，　６１　通信部，　６２　SAM，　６３　伸張部，　７１　相互認証モジュール，　７２　課金処理モジュール，　７３　記憶モジュール，　７４　復号／暗号化モジュール，　７５　相互認証モジュール，　７６　復号モジュール，　７７　復号モジュール，　８１　相互認証モジュール，　９１　復号ユニット，　９２　暗号化ユニット，　９３　暗号化ユニット，　１０１　相互認証モジュール，　１０２　復号モジュール，　１０３　復号モジュール

【図１】

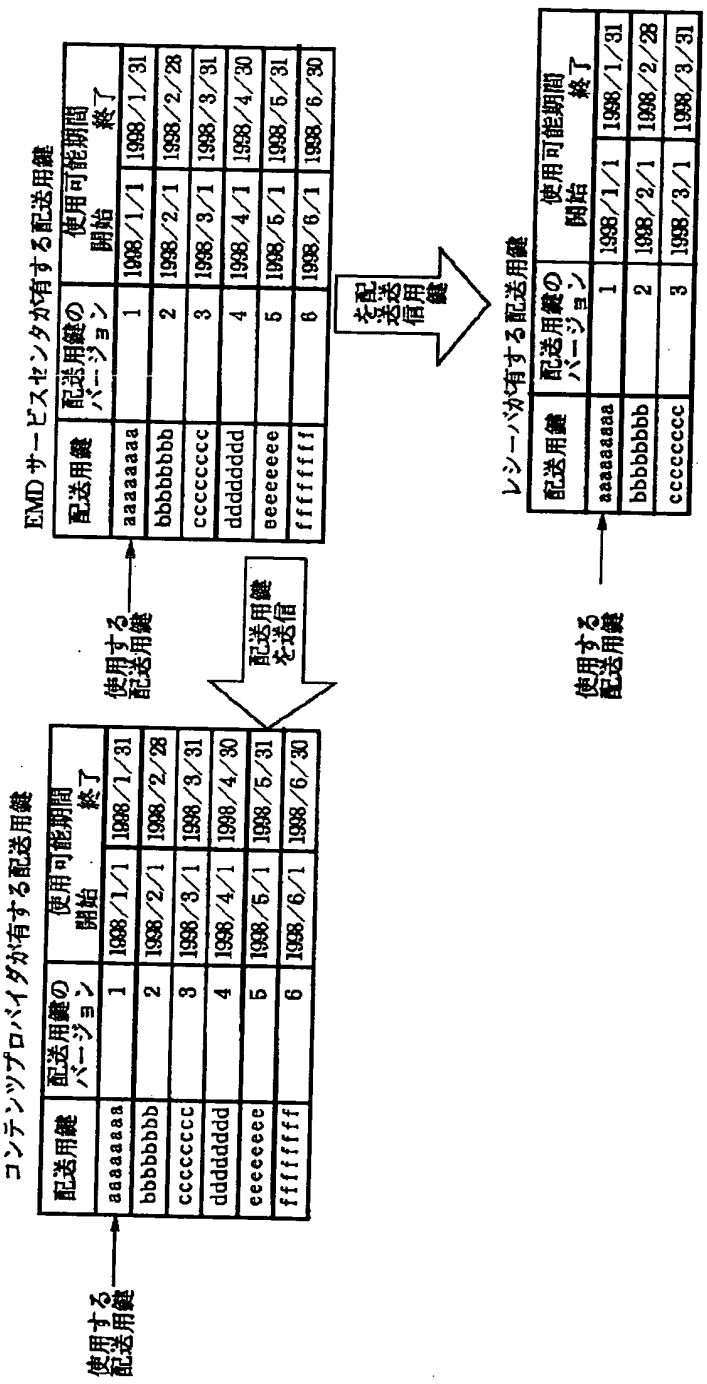


【図２】

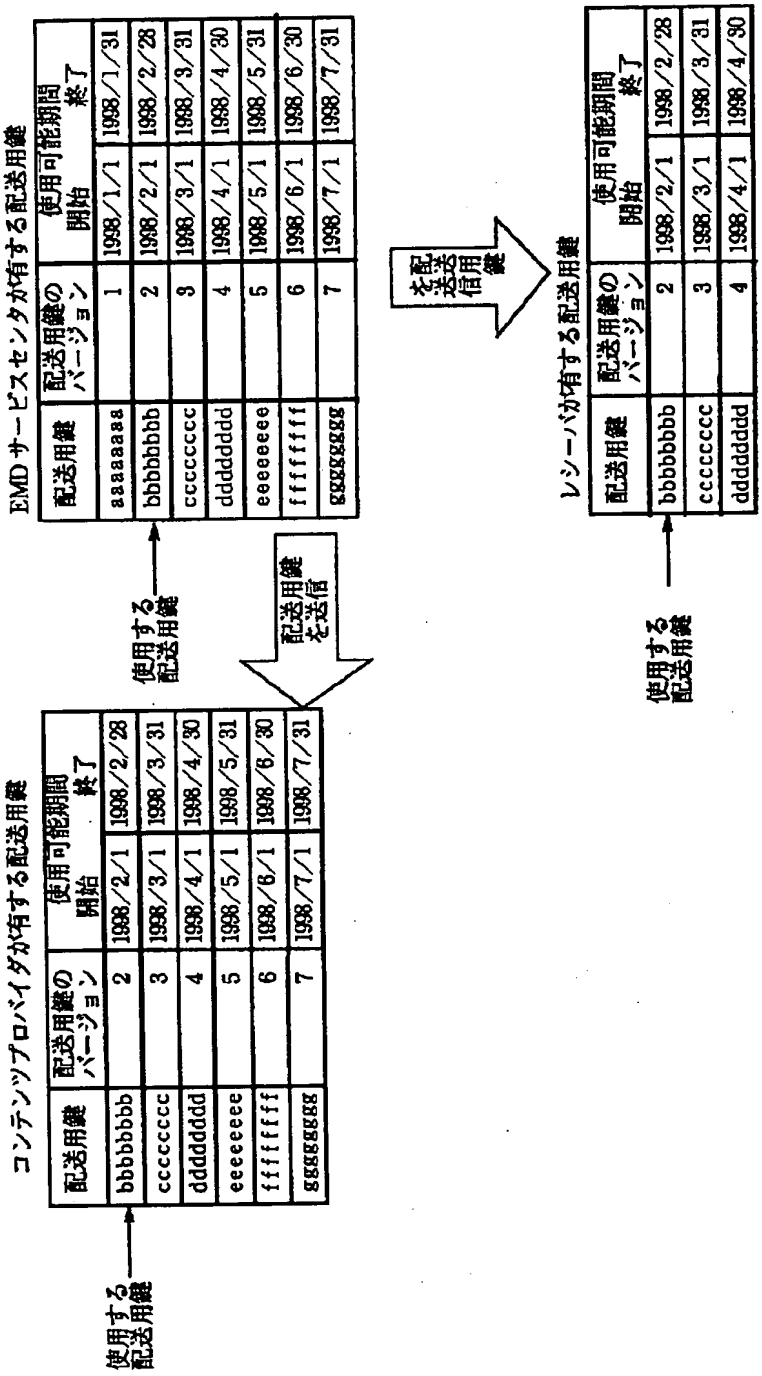


EMD サービスセンタ 1

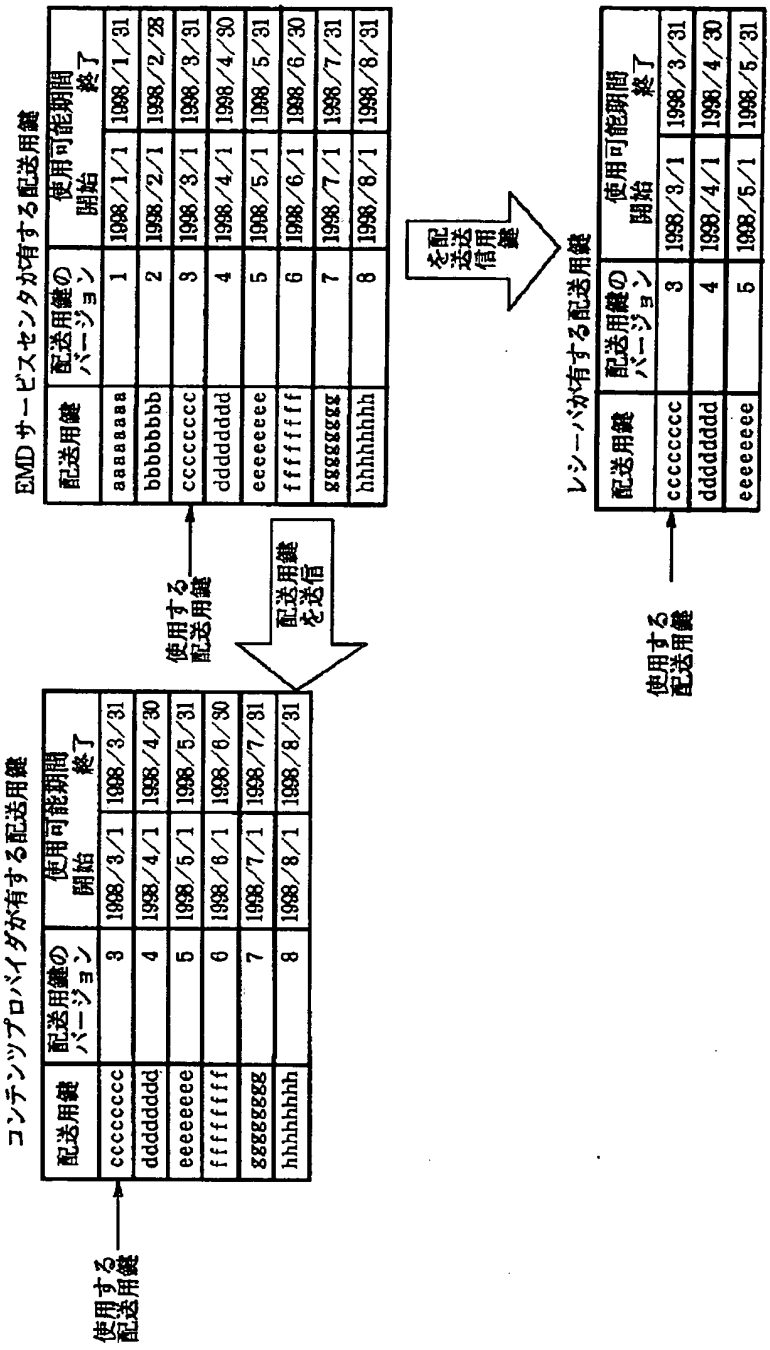
【図３】


コンテンツプロバイダが有する配送用鍵
配送用鍵
配送用鍵のバージョン
使用可能期間 開始
使用可能期間 終了
aaaaaaaa 1 1998/1/1 1998/1/31
bbbbbbbb 2 1998/2/1 1998/2/28
cccccccc 3 1998/3/1 1998/3/31
dddddddd 4 1998/4/1 1998/4/30
eeeeeeee 5 1998/5/1 1998/5/31
ffffffff 6 1998/6/1 1998/6/30
使用する配送用鍵
配送用鍵を送信
EMDサービスセンタが有する配送用鍵
配送用鍵
配送用鍵のバージョン
使用可能期間 開始
使用可能期間 終了
aaaaaaaa 1 1998/1/1 1998/1/31
bbbbbbbb 2 1998/2/1 1998/2/28
cccccccc 3 1998/3/1 1998/3/31
dddddddd 4 1998/4/1 1998/4/30
eeeeeeee 5 1998/5/1 1998/5/31
ffffffff 6 1998/6/1 1998/6/30
使用する配送用鍵
配送用鍵を送信
レシーバが有する配送用鍵
配送用鍵
配送用鍵のバージョン
使用可能期間 開始
使用可能期間 終了
aaaaaaaa 1 1998/1/1 1998/1/31
bbbbbbbb 2 1998/2/1 1998/2/28
cccccccc 3 1998/3/1 1998/3/31
使用する配送用鍵

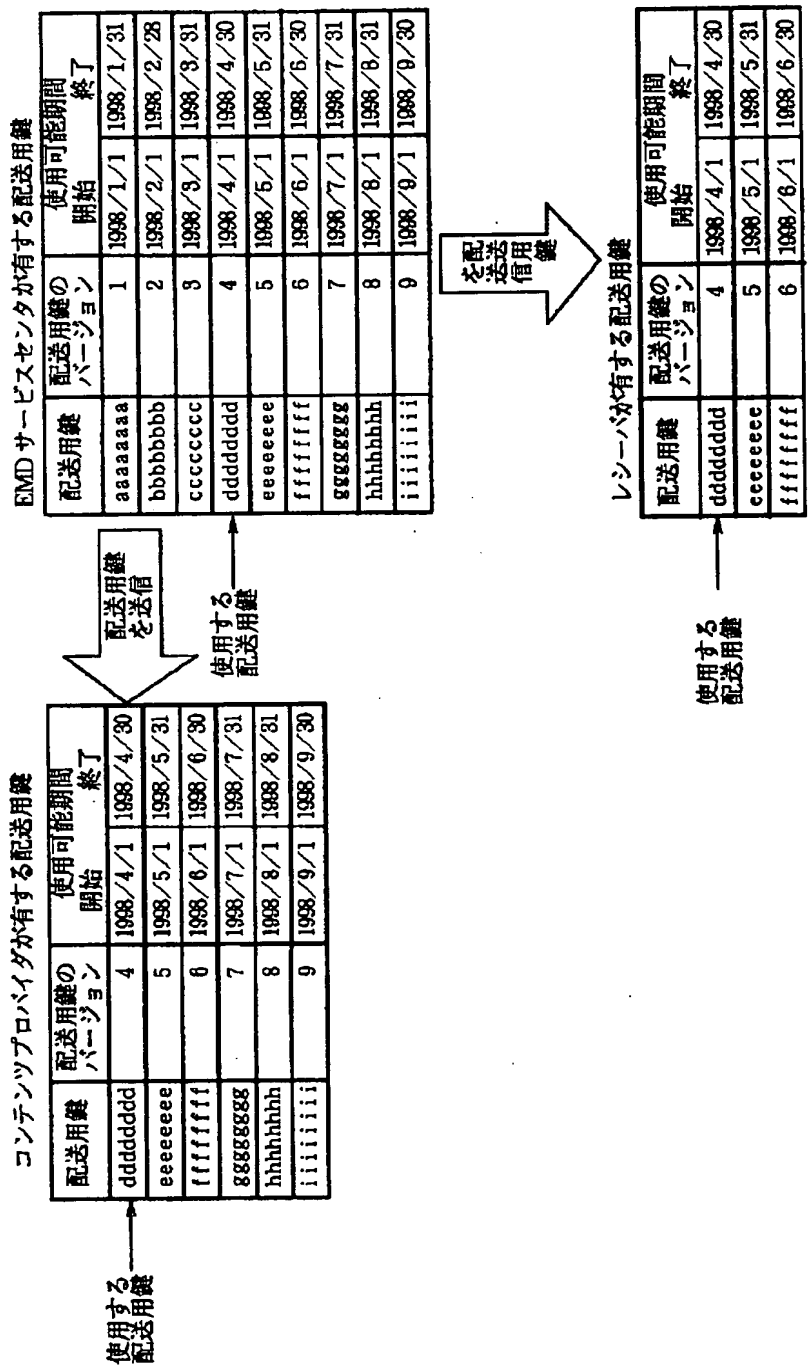
【図４】


コンテンツプロバイダが有する配送用鍵
配送用鍵 | 配送用鍵のバージョン | 使用可能期間 開始 | 使用可能期間 終了
bbbbbbbb | 2 | 1998/2/1 | 1998/2/28
cccccccc | 3 | 1998/3/1 | 1998/3/31
dddddddd | 4 | 1998/4/1 | 1998/4/30
eeeeeeee | 5 | 1998/5/1 | 1998/5/31
ffffffff | 6 | 1998/6/1 | 1998/6/30
gggggggg | 7 | 1998/7/1 | 1998/7/31
使用する配送用鍵
配送用鍵を送信
EMDサービスセンタが有する配送用鍵
配送用鍵 | 配送用鍵のバージョン | 使用可能期間 開始 | 使用可能期間 終了
aaaaaaaa | 1 | 1998/1/1 | 1998/1/31
bbbbbbbb | 2 | 1998/2/1 | 1998/2/28
cccccccc | 3 | 1998/3/1 | 1998/3/31
dddddddd | 4 | 1998/4/1 | 1998/4/30
eeeeeeee | 5 | 1998/5/1 | 1998/5/31
ffffffff | 6 | 1998/6/1 | 1998/6/30
gggggggg | 7 | 1998/7/1 | 1998/7/31
使用する配送用鍵
を配送信用鍵
レシーバが有する配送用鍵
配送用鍵 | 配送用鍵のバージョン | 使用可能期間 開始 | 使用可能期間 終了
bbbbbbbb | 2 | 1998/2/1 | 1998/2/28
cccccccc | 3 | 1998/3/1 | 1998/3/31
dddddddd | 4 | 1998/4/1 | 1998/4/30
使用する配送用鍵

【図５】


EMDサービスセンタが有する配送用鍵
配送用鍵
配送用鍵のバージョン
使用可能期間 開始
使用可能期間 終了
aaaaaaaa 1 1998/1/1 1998/1/31
bbbbbbbb 2 1998/2/1 1998/2/28
cccccccc 3 1998/3/1 1998/3/31
dddddddd 4 1998/4/1 1998/4/30
eeeeeeee 5 1998/5/1 1998/5/31
ffffffff 6 1998/6/1 1998/6/30
gggggggg 7 1998/7/1 1998/7/31
hhhhhhhh 8 1998/8/1 1998/8/31
使用する配送用鍵
配送用鍵を送信
を配送信用鍵
レシーバが有する配送用鍵
配送用鍵
配送用鍵のバージョン
使用可能期間 開始
使用可能期間 終了
cccccccc 3 1998/3/1 1998/3/31
dddddddd 4 1998/4/1 1998/4/30
eeeeeeee 5 1998/5/1 1998/5/31
使用する配送用鍵
コンテンツプロバイダが有する配送用鍵
配送用鍵
配送用鍵のバージョン
使用可能期間 開始
使用可能期間 終了
cccccccc 3 1998/3/1 1998/3/31
dddddddd 4 1998/4/1 1998/4/30
eeeeeeee 5 1998/5/1 1998/5/31
ffffffff 6 1998/6/1 1998/6/30
gggggggg 7 1998/7/1 1998/7/31
hhhhhhhh 8 1998/8/1 1998/8/31
使用する配送用鍵

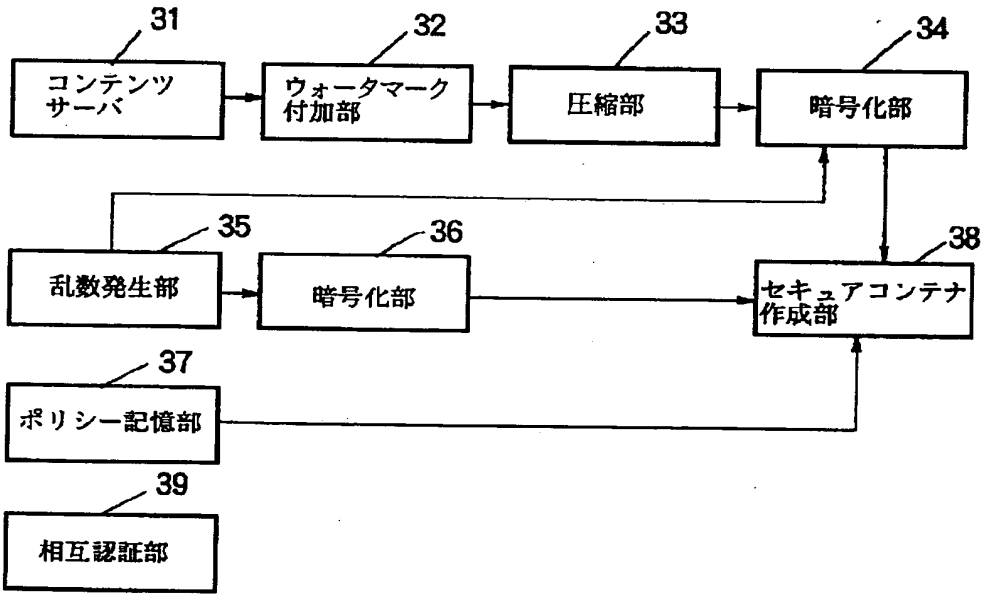
【図６】


コンテンツプロバイダが有する配送用鍵
配送用鍵
配送用鍵のバージョン
使用可能期間 開始
終了
dddddddd 4 1998/4/1 1998/4/30
eeeeeeee 5 1998/5/1 1998/5/31
ffffffff 6 1998/6/1 1998/6/30
gggggggg 7 1998/7/1 1998/7/31
hhhhhhhh 8 1998/8/1 1998/8/31
iiiiiiiii 9 1998/9/1 1998/9/30
使用する配送用鍵
配送用鍵を送信
EMDサービスセンタが有する配送用鍵
配送用鍵
配送用鍵のバージョン
使用可能期間 開始
終了
aaaaaaaa 1 1998/1/1 1998/1/31
bbbbbbbb 2 1998/2/1 1998/2/28
cccccccc 3 1998/3/1 1998/3/31
dddddddd 4 1998/4/1 1998/4/30
eeeeeeee 5 1998/5/1 1998/5/31
ffffffff 6 1998/6/1 1998/6/30
gggggggg 7 1998/7/1 1998/7/31
hhhhhhhh 8 1998/8/1 1998/8/31
iiiiiiiii 9 1998/9/1 1998/9/30
使用する配送用鍵
を配送信用鍵
レシーバが有する配送用鍵
配送用鍵
配送用鍵のバージョン
使用可能期間 開始
終了
dddddddd 4 1998/4/1 1998/4/30
eeeeeeee 5 1998/5/1 1998/5/31
ffffffff 6 1998/6/1 1998/6/30
使用する配送用鍵

【図７】

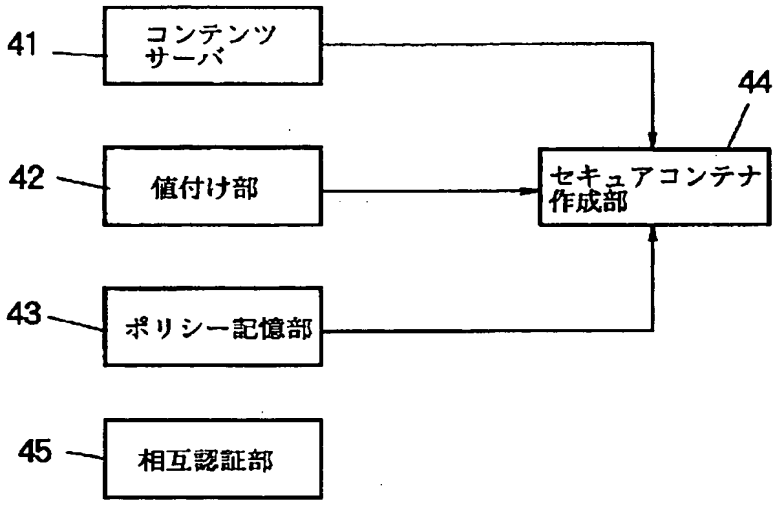
ID	決済処理	登録	EMDサービスセンタとの接続
0000000000000001h	可	可	可
0000000000000002h	可	可	不可
0000000000000003h	可	不可	可
0000000000000004h	可	不可	不可
0000000000000005h	不可	可	可
0000000000000006h	不可	可	不可
0000000000000007h	不可	不可	可
0000000000000008h	不可	不可	不可
0000000000000009h	可	可	可
・・・			
FFFFFFFFFFFFFFFEh	可	不可	不可
FFFFFFFFFFFFFFFFh	不可	可	可

【図８】

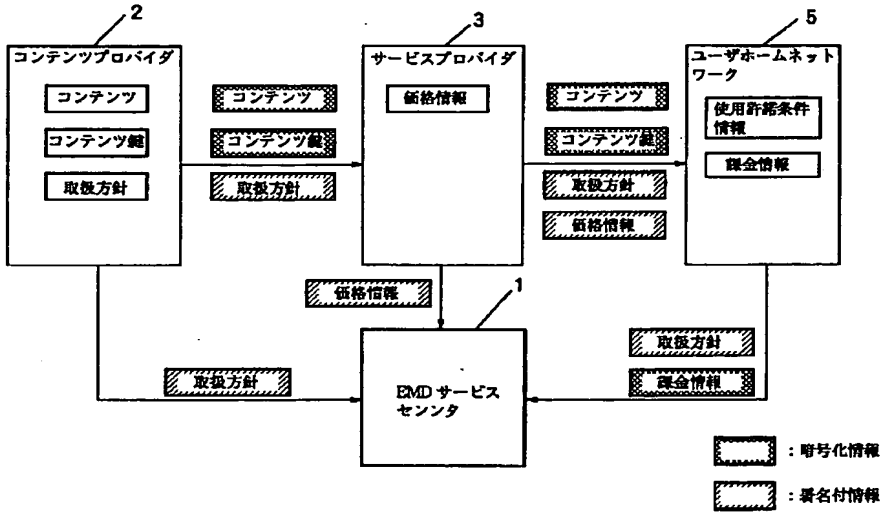


コンテンツプロバイダ 2

【図９】



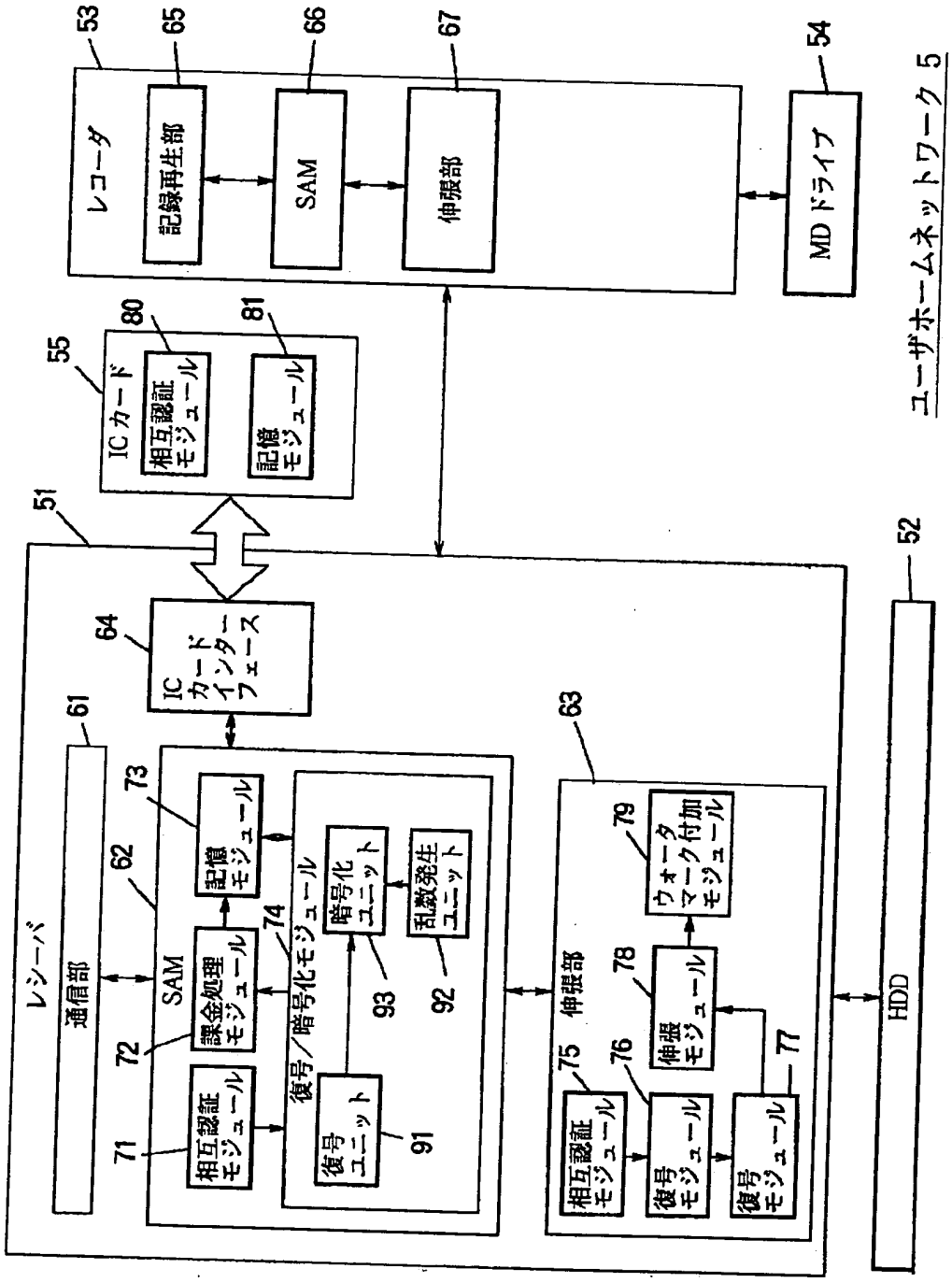
【図１２】



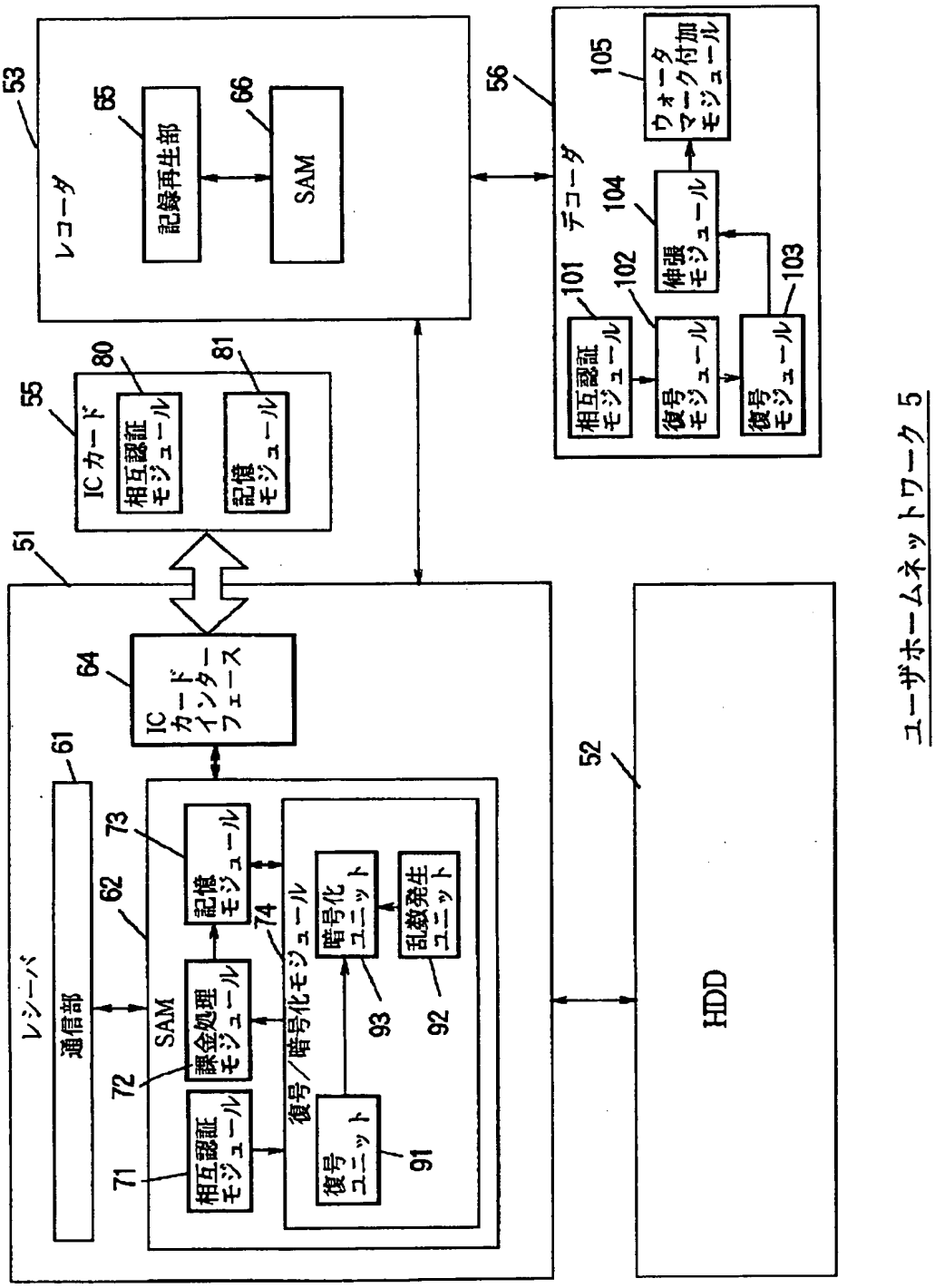
【図２８】

コンテンツ ID	コンテンツプロバイダ ID	権利団体
1	201	10%
2	201	20%

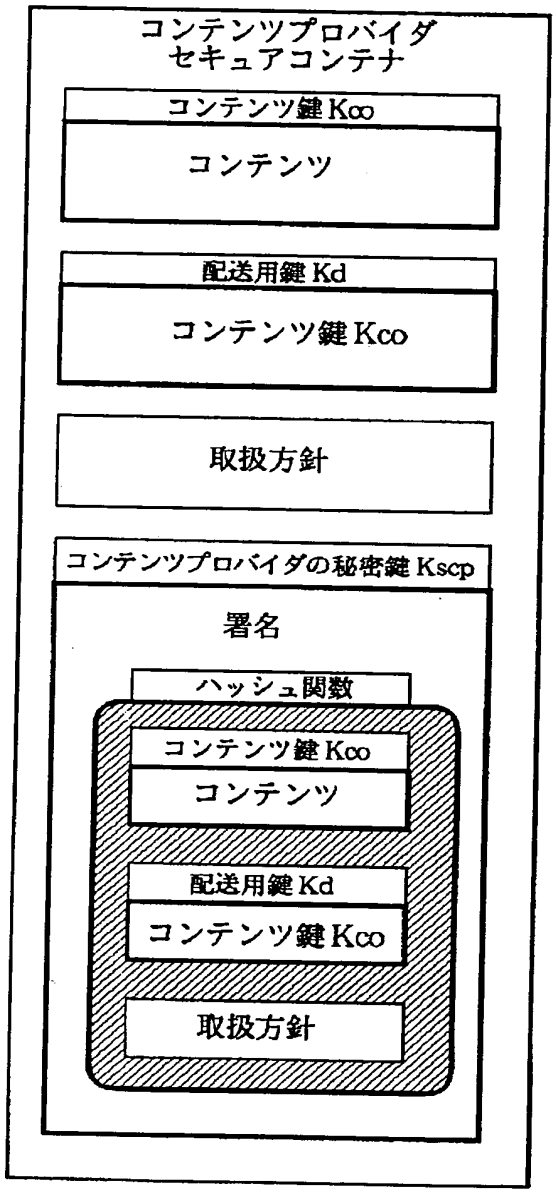
【図１０】


ユーザホームネットワーク 5
レコーダ
記録再生部
SAM
伸張部
MD ドライブ
ICカード
相互認証モジュール
記憶モジュール
ICカードインターフェース
レシーバ
通信部
SAM
課金処理モジュール
相互認証モジュール
記憶モジュール
暗号化／暗号化モジュール
復号ユニット
暗号化ユニット
乱数発生ユニット
伸張部
相互認証モジュール
復号モジュール
伸張モジュール
復号モジュール
ウォータマーク付加モジュール
HDD
51
52
53
54
55
61
62
63
64
65
66
67
71
72
73
74
75
76
77
78
79
80
81
91
92
93

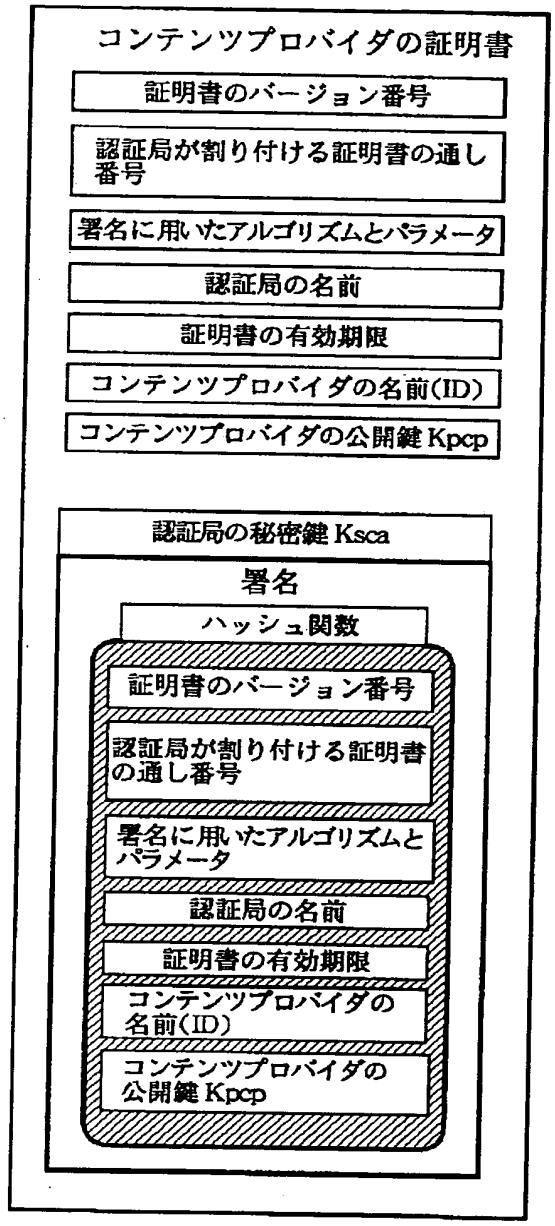
【図１１】


ユーザホームネットワーク 5
レコーダ
53
記録再生部
65
SAM
66
デコーダ
56
ウォータマーク付加モジュール
105
伸張モジュール
104
相互認証モジュール
101
復号モジュール
102
復号モジュール
103
ICカード
55
相互認証モジュール
80
記憶モジュール
81
51
ICカードインターフェース
64
レシーバ
61
通信部
62
SAM
課金処理モジュール
72
相互認証モジュール
71
記憶モジュール
73
復号／暗号化モジュール
74
復号ユニット
91
暗号化ユニット
93
乱数発生ユニット
92
52
HDD

【図１３】



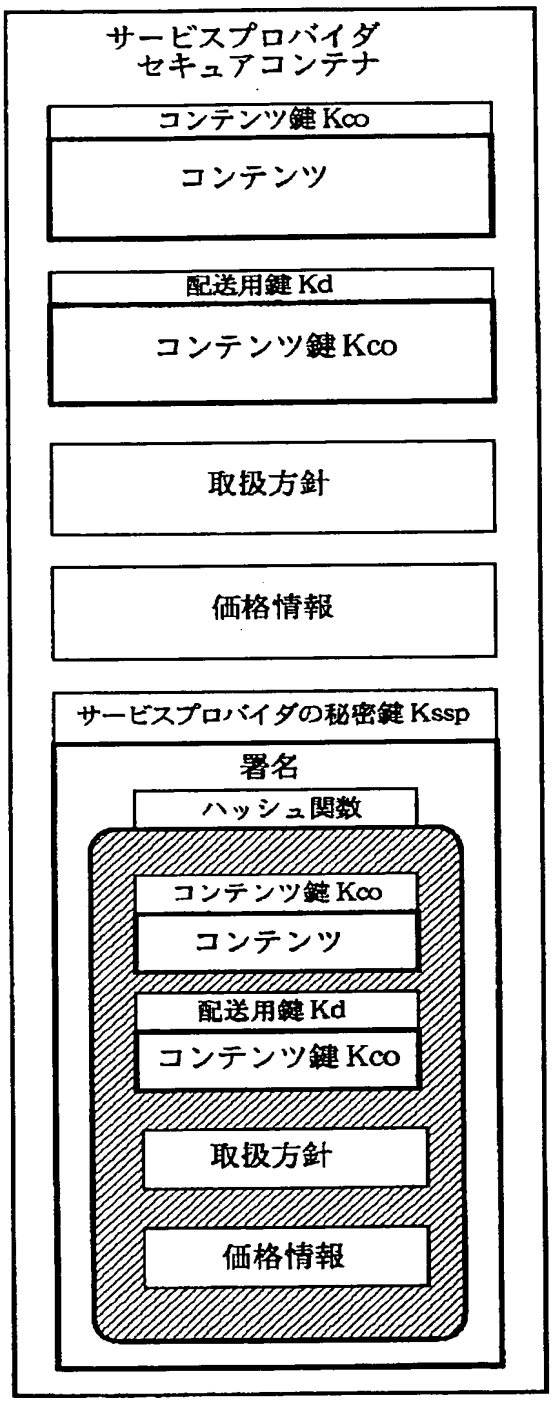
【図１４】



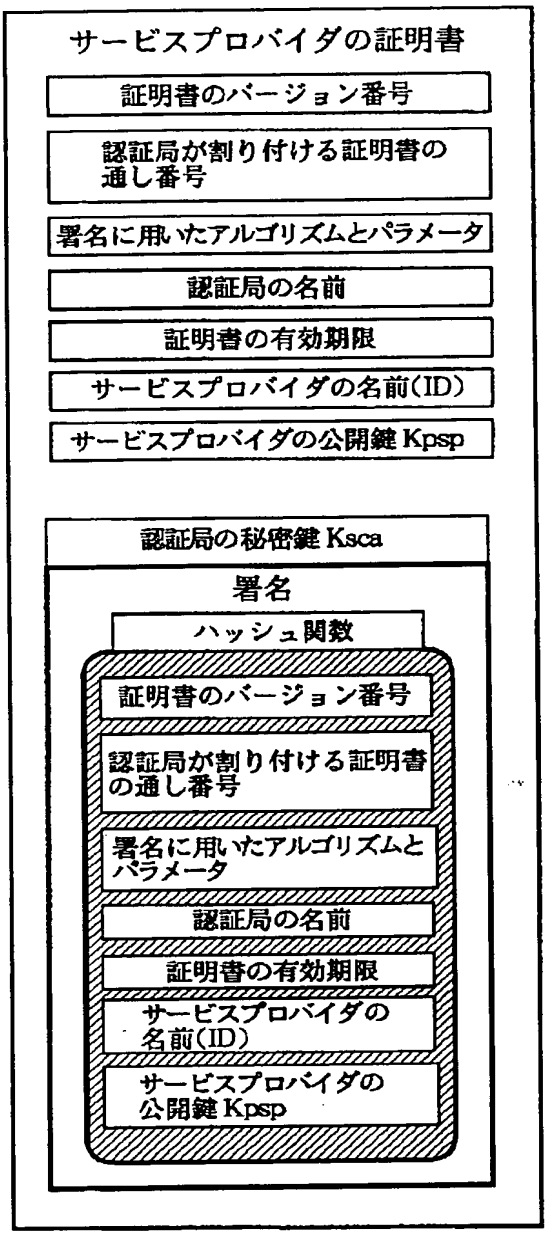
【図２９】

プロバイダ ID	コンテンツ ID	割引率	期間
コンテンツプロバイダ１	1	0.02	1998.9～1998.12
	2	0.03	
	すべてのコンテンツ	0.01	
コンテンツプロバイダ２	3	0.05	
サービスプロバイダ１	1	0.03	
サービスプロバイダ２	4	0.01	

【図１５】



【図１６】



【図３０】

月額固定額	変動額		
1000円	期間	1998. 8.～1998. 9	－10%
	利用料	3000円以上	－5%

【図１７】

(A) 取扱方針

利用内容	再生	シングルコピー	マルチコピー
可／否	1	0	1

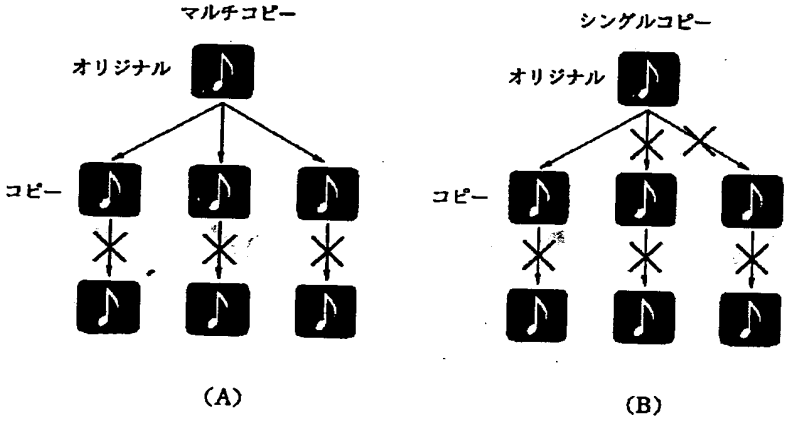
(B) 取扱方針および価格情報

利用内容	再生	シングルコピー	マルチコピー
可／否	1	0	1
価格	150円	−	80円

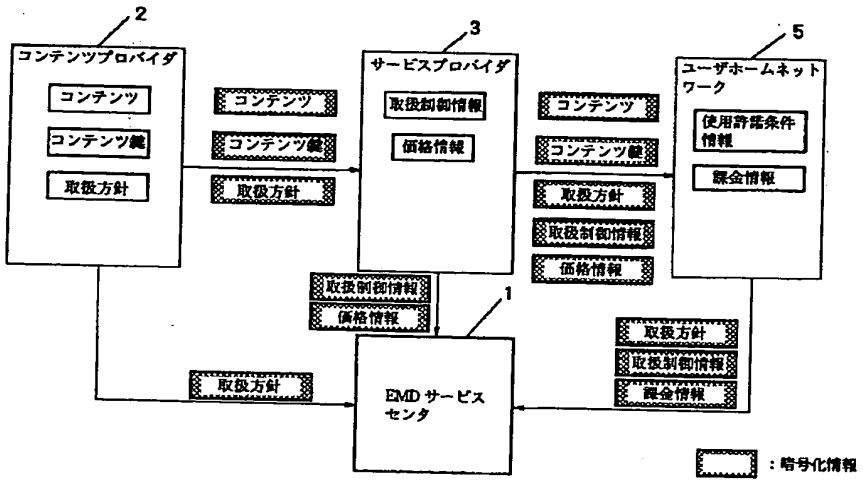
(C) 使用許諾条件情報

利用内容	再生	シングルコピー	マルチコピー
可／否	1	0	0

【図１８】



【図２４】



【図５８】

(A)
クレジット決済オブジェクト1
支払元：ユーザのID
徴収額：x
支払先：サービスプロバイダのID
支払額：x1

(B)
クレジット決済オブジェクト2
支払元：クレジット決済オブジェクト1
徴収額：−
支払先：コンテンツプロバイダのID
支払額：x2

(C)
クレジット決済オブジェクト3
支払元：クレジット決済オブジェクト1
徴収額：−
支払先：権利団体のID
支払額：x3

(D)
クレジット決済オブジェクト4
支払元：クレジット決済オブジェクト1
徴収額：−
支払先：EMDサービスセンタのID
支払額：x4

【図５９】

(A)
銀行決済オブジェクト1
支払元：サービスプロバイダのID
徴収額：y1
支払先：EMDサービスセンタのID
支払額：y1

(B)
銀行決済オブジェクト2
支払元：コンテンツプロバイダのID
徴収額：y2
支払先：EMDサービスセンタのID
支払額：y2

(C)
銀行決済オブジェクト3
支払元：権利団体のID
徴収額：y3
支払先：EMDサービスセンタのID
支払額：y3

【図１９】

(A) 取扱方針 利益分配

利用内容	再生	シングルコピー	マルチコピー
可／否	1	0	1
利益分配	70円	－	40円

(B) 取扱方針 利益分配 価格情報

利用内容	再生	シングルコピー	マルチコピー
可／否	1	0	1
利益分配	60円	－	30円
分配価格	150円	－	80円

(C) 課金情報

利用内容	再生	シングルコピー	マルチコピー
利用回数	1	0	0

【図２０】

(A) 取扱方針 および 価格情報

利用内容	再生		
	制限なし	回数制限	期日制限
	－	5	1998／12／31
価格	－	60円	90円

(B) 使用許諾条件 情報

利用内容	再生		
	制限なし	回数制限	期日制限
	－	5	－

3回再生後

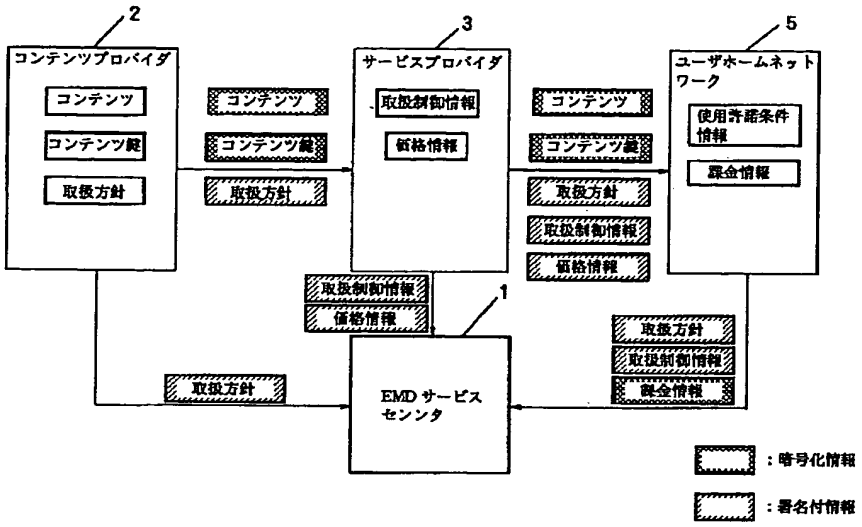
(C) 使用許諾条件 情報

利用内容	再生		
	制限なし	回数制限	期日制限
	－	2	－

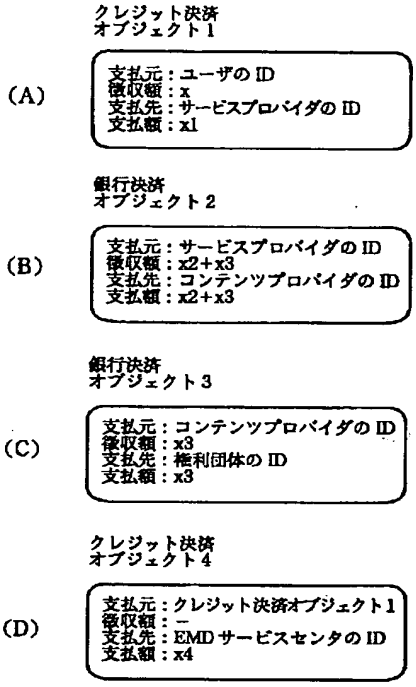
【図４２】

SAMのID (64bit)	登録拒絶フラグ (1bit)	ステータスフラグ (4bit)	コンディションフラグ (ibit)	署名
0000000000000001h	1	0000	0	xxxxxxxxx
0000000000000002h	1	1010	1	xxxxxxxxx
0000000000000003h	1	1100	1	xxxxxxxxx
000000000000000Ah	0	0000	1	xxxxxxxxx

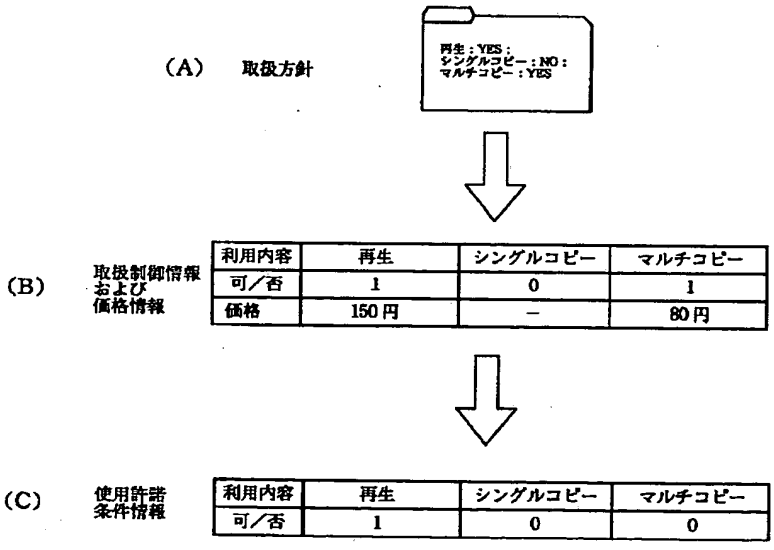
【図２１】



【図６０】



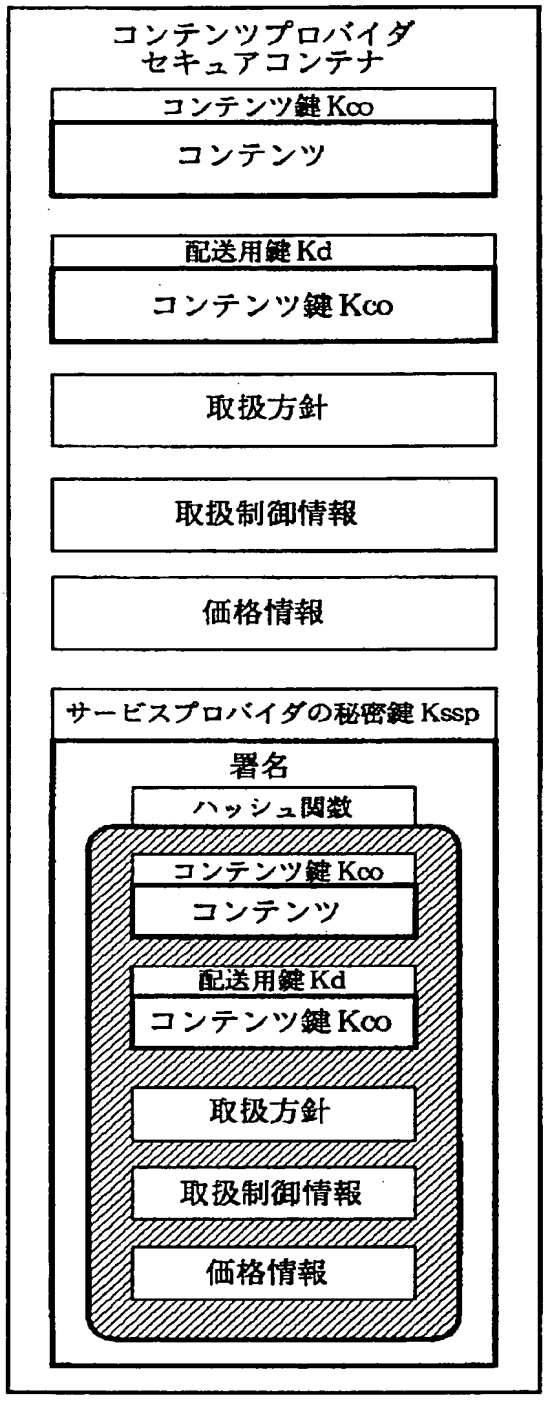
【図２３】



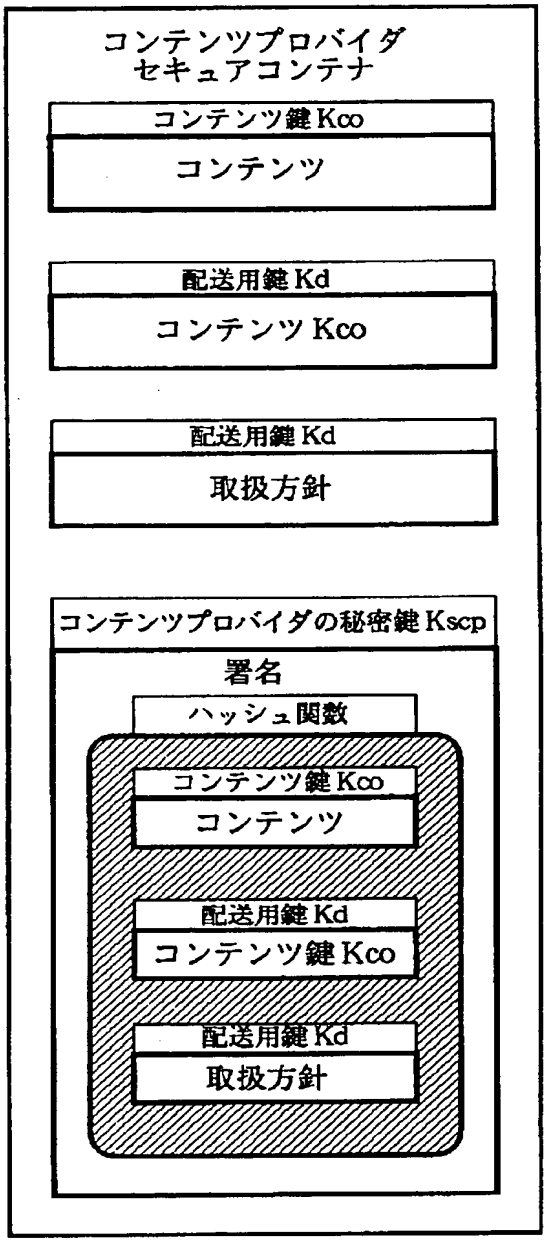
利用内容	再生	シングルコピー	マルチコピー
可／否	1	0	1
価格	150 円	－	80 円

利用内容	再生	シングルコピー	マルチコピー
可／否	1	0	0

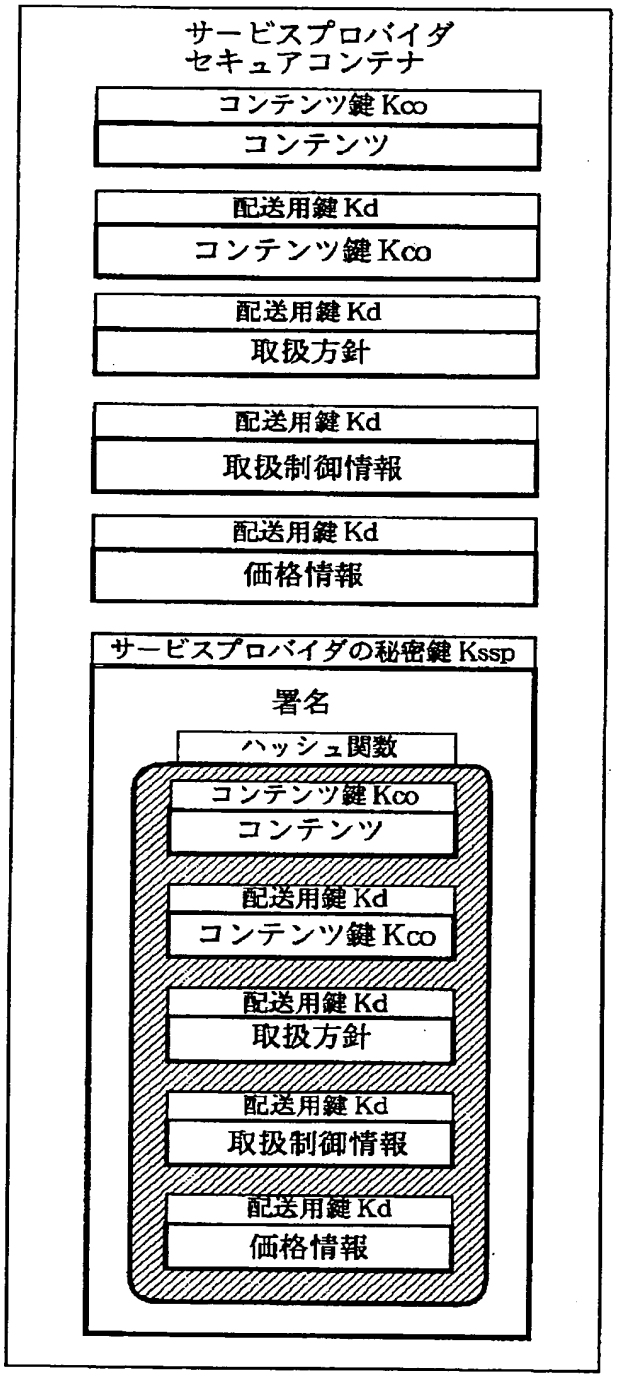
【図２２】


コンテンツプロバイダ
セキュアコンテナ
コンテンツ鍵 Kco
コンテンツ
配送用鍵 Kd
コンテンツ鍵 Kco
取扱方針
取扱制御情報
価格情報
サービスプロバイダの秘密鍵 Kssp
署名
ハッシュ関数
コンテンツ鍵 Kco
コンテンツ
配送用鍵 Kd
コンテンツ鍵 Kco
取扱方針
取扱制御情報
価格情報

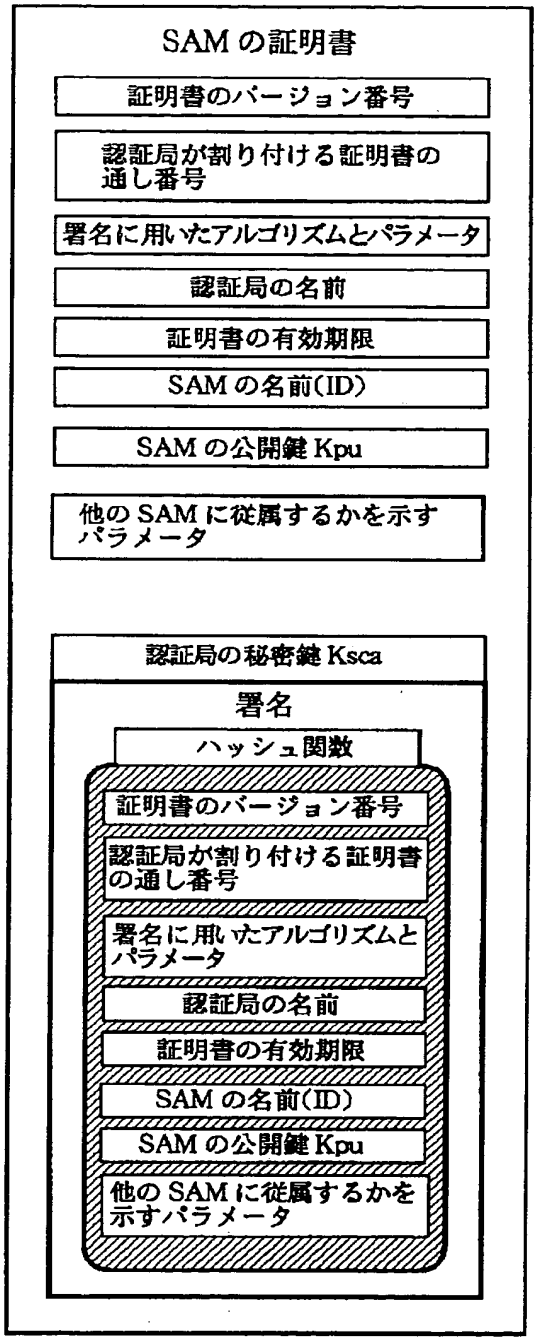
【図２５】


コンテンツプロバイダ
セキュアコンテナ
コンテンツ鍵 Kco
コンテンツ
配送用鍵 Kd
コンテンツ Kco
配送用鍵 Kd
取扱方針
コンテンツプロバイダの秘密鍵 Kscp
署名
ハッシュ関数
コンテンツ鍵 Kco
コンテンツ
配送用鍵 Kd
コンテンツ鍵 Kco
配送用鍵 Kd
取扱方針

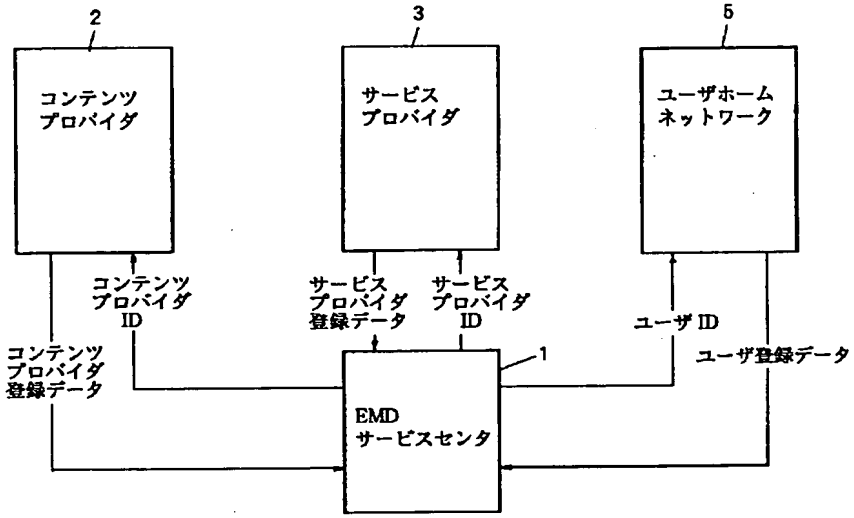
【図２６】


サービスプロバイダ
セキュアコンテナ
コンテンツ鍵 Kco
コンテンツ
配送用鍵 Kd
コンテンツ鍵 Kco
配送用鍵 Kd
取扱方針
配送用鍵 Kd
取扱制御情報
配送用鍵 Kd
価格情報
サービスプロバイダの秘密鍵 Kssp
署名
ハッシュ関数
コンテンツ鍵 Kco
コンテンツ
配送用鍵 Kd
コンテンツ鍵 Kco
配送用鍵 Kd
取扱方針
配送用鍵 Kd
取扱制御情報
配送用鍵 Kd
価格情報

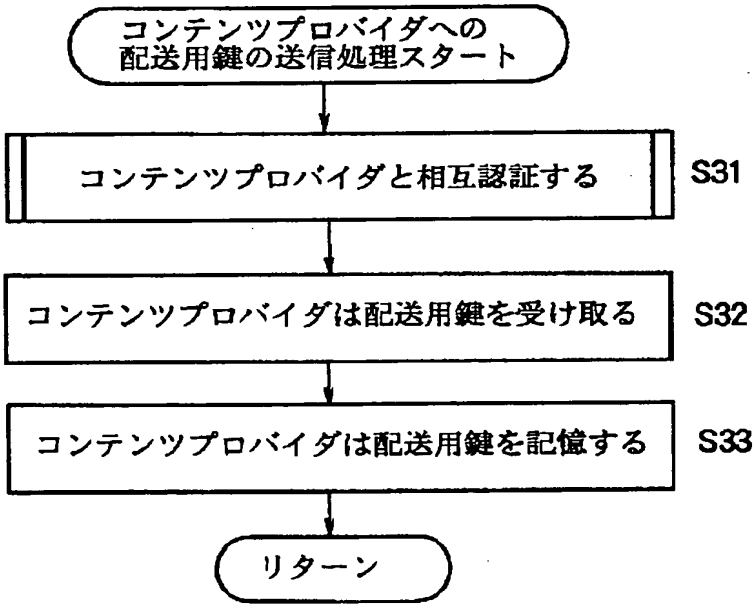
【図４１】


SAM の証明書
証明書のバージョン番号
認証局が割り付ける証明書の通し番号
署名に用いたアルゴリズムとパラメータ
認証局の名前
証明書の有効期限
SAM の名前(ID)
SAM の公開鍵 Kpu
他の SAM に従属するかを示すパラメータ
認証局の秘密鍵 Ksca
署名
ハッシュ関数
証明書のバージョン番号
認証局が割り付ける証明書の通し番号
署名に用いたアルゴリズムとパラメータ
認証局の名前
証明書の有効期限
SAM の名前(ID)
SAM の公開鍵 Kpu
他の SAM に従属するかを示すパラメータ

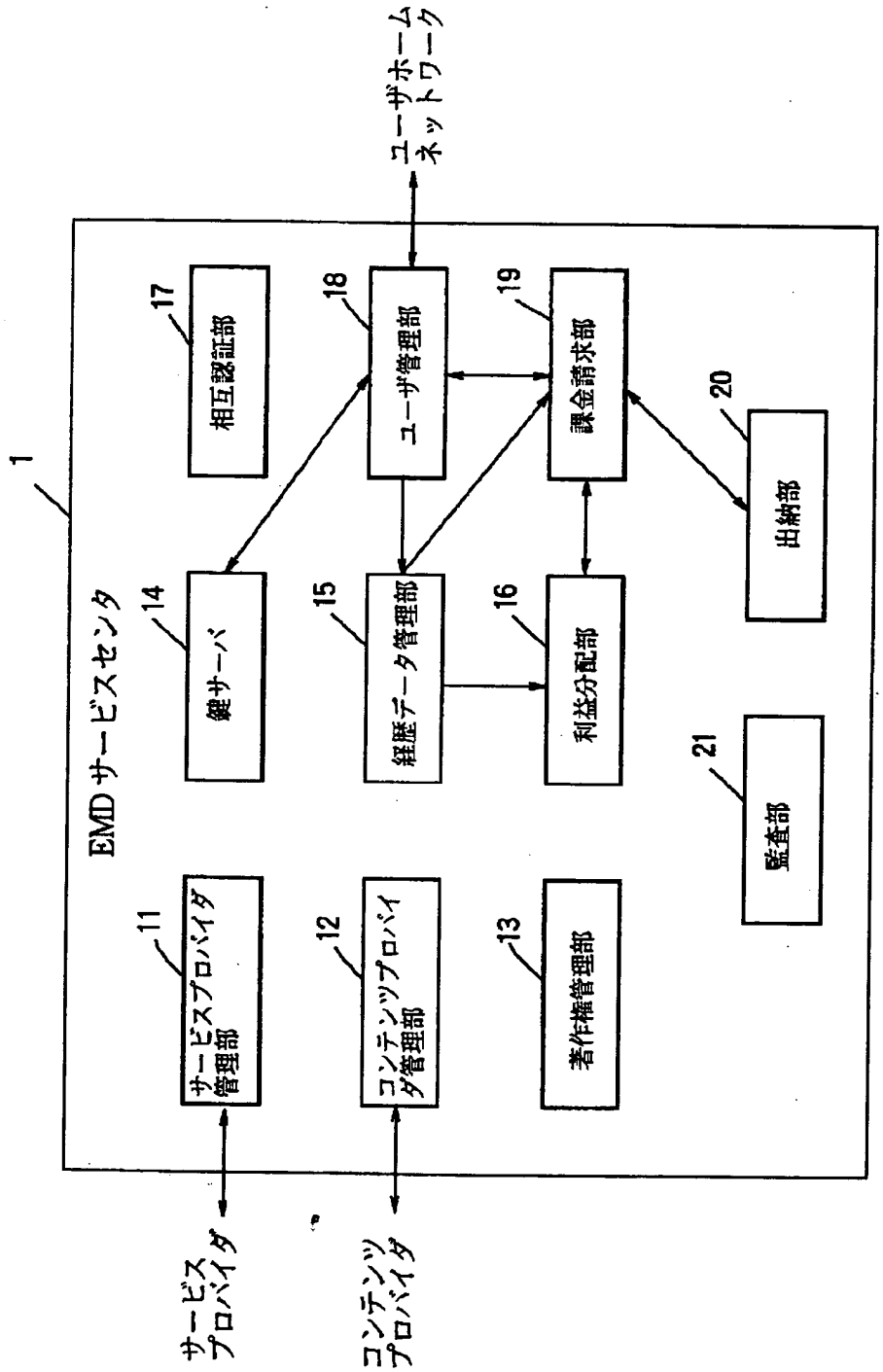
【図２７】


2
3
5
コンテンツ
プロバイダ
サービス
プロバイダ
ユーザホーム
ネットワーク
コンテンツ
プロバイダ
ID
サービス
プロバイダ
登録データ
サービス
プロバイダ
ID
ユーザ ID
コンテンツ
プロバイダ
登録データ
1
ユーザ登録データ
EMD
サービスセンタ

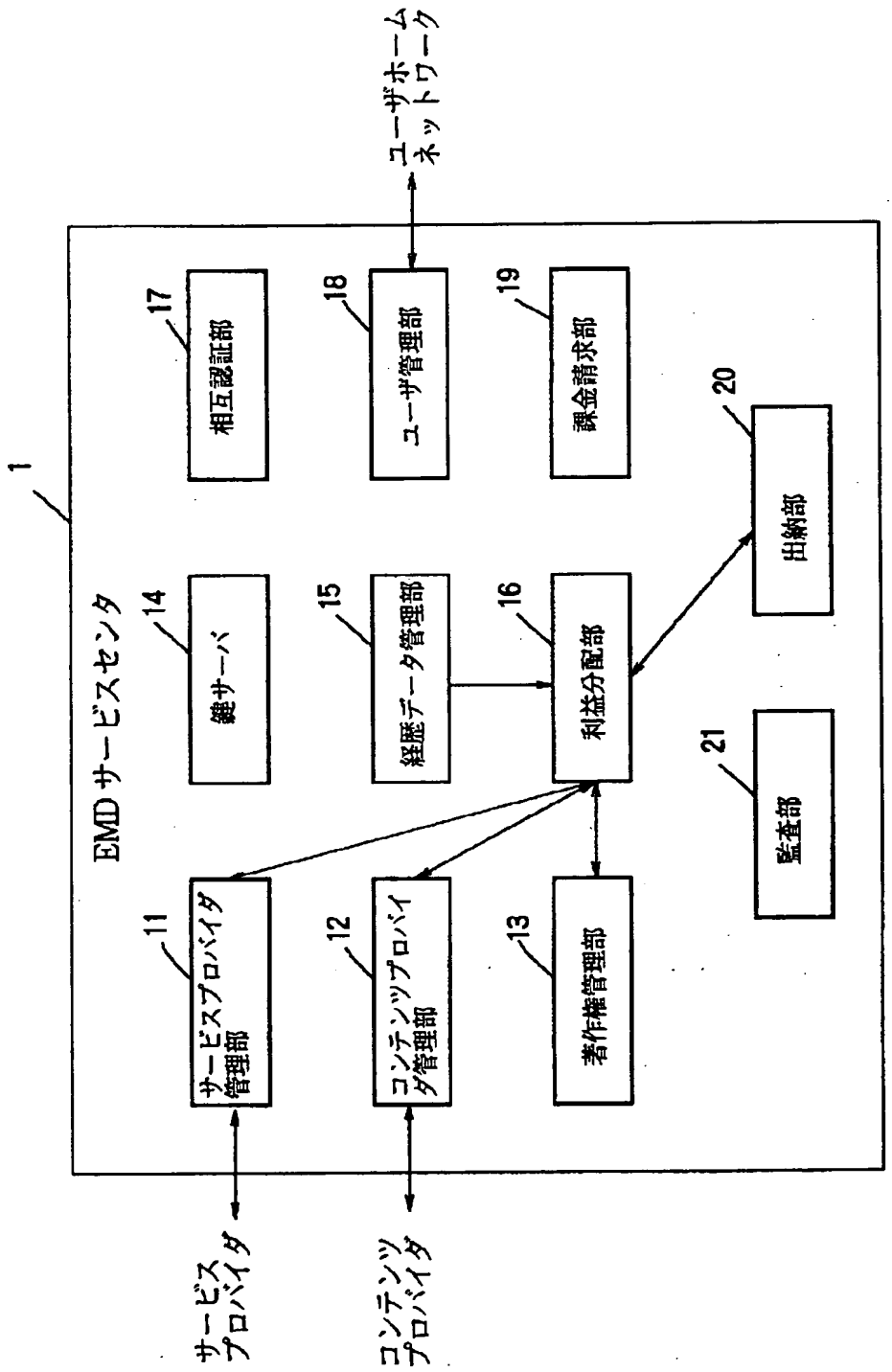
【図３６】


コンテンツプロバイダへの
配送用鍵の送信処理スタート
コンテンツプロバイダと相互認証する
S31
コンテンツプロバイダは配送用鍵を受け取る
S32
コンテンツプロバイダは配送用鍵を記憶する
S33
リターン

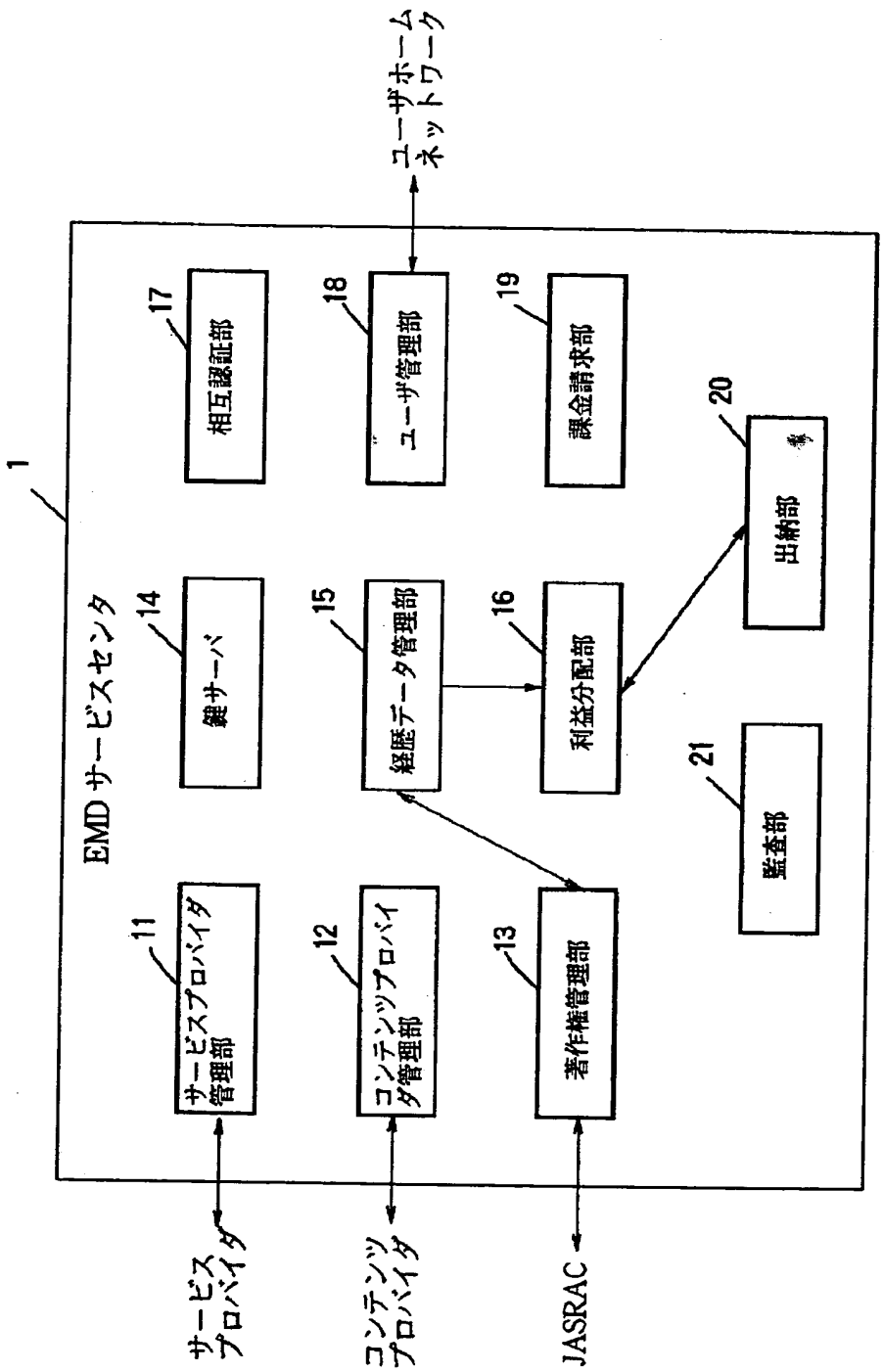
【図３１】


ユーザホームネットワーク
1
EMDサービスセンタ
17
相互認証部
18
ユーザ管理部
19
課金請求部
20
出納部
14
鍵サーバ
15
経歴データ管理部
16
利益分配部
21
監査部
11
サービスプロバイダ管理部
12
コンテンツプロバイダ管理部
13
著作権管理部
サービスプロバイダ
コンテンツプロバイダ

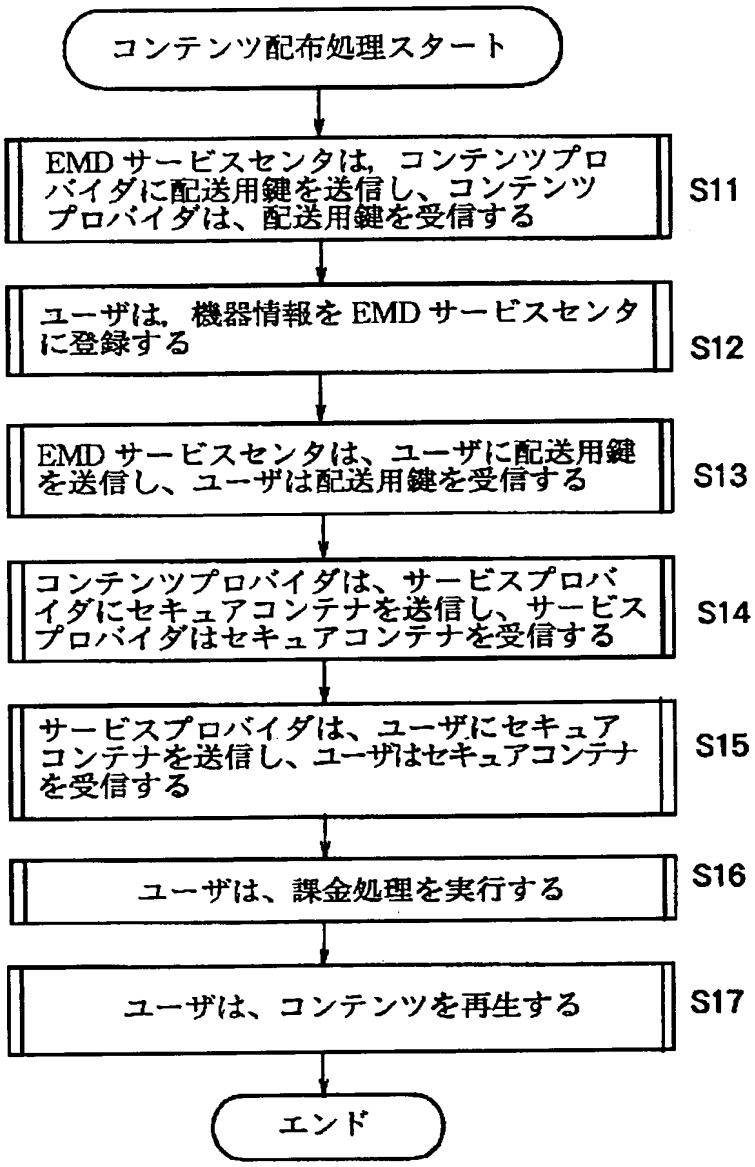
【図３２】


ユーザホーム
ネットワーク
1
EMD サービスセンタ
17
相互認証部
18
ユーザ管理部
19
課金請求部
20
出納部
14
鍵サーバ
15
経歴データ管理部
16
利益分配部
21
監査部
11
サービスプロバイダ
管理部
12
コンテンツプロバイ
ダ管理部
13
著作権管理部
サービス
プロバイダ
コンテンツ
プロバイダ

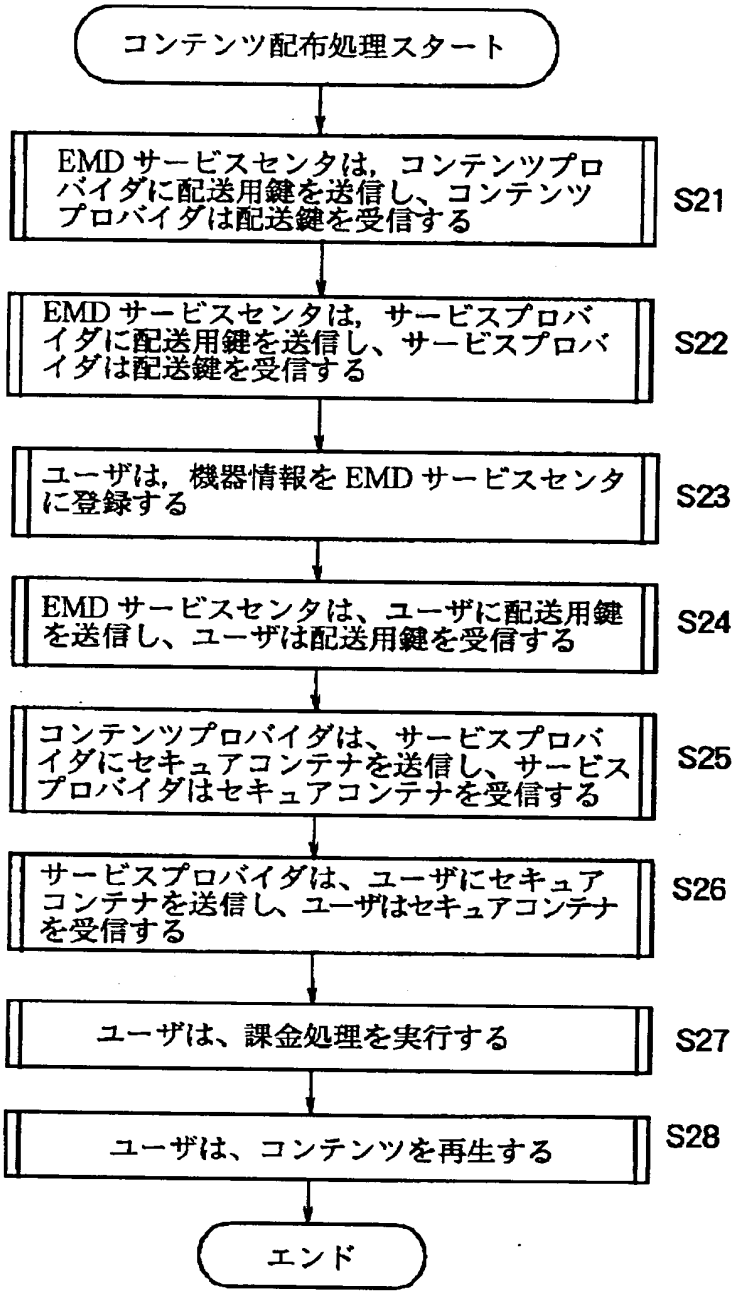
【図３３】


ユーザホームネットワーク
1
EMD サービスセンタ
17
相互認証部
18
ユーザ管理部
19
課金請求部
20
出納部
14
鍵サーバ
15
経歴データ管理部
16
利益分配部
21
監査部
11
サービスプロバイダ管理部
12
コンテンツプロバイダ管理部
13
著作権管理部
サービスプロバイダ
コンテンツプロバイダ
JASRAC

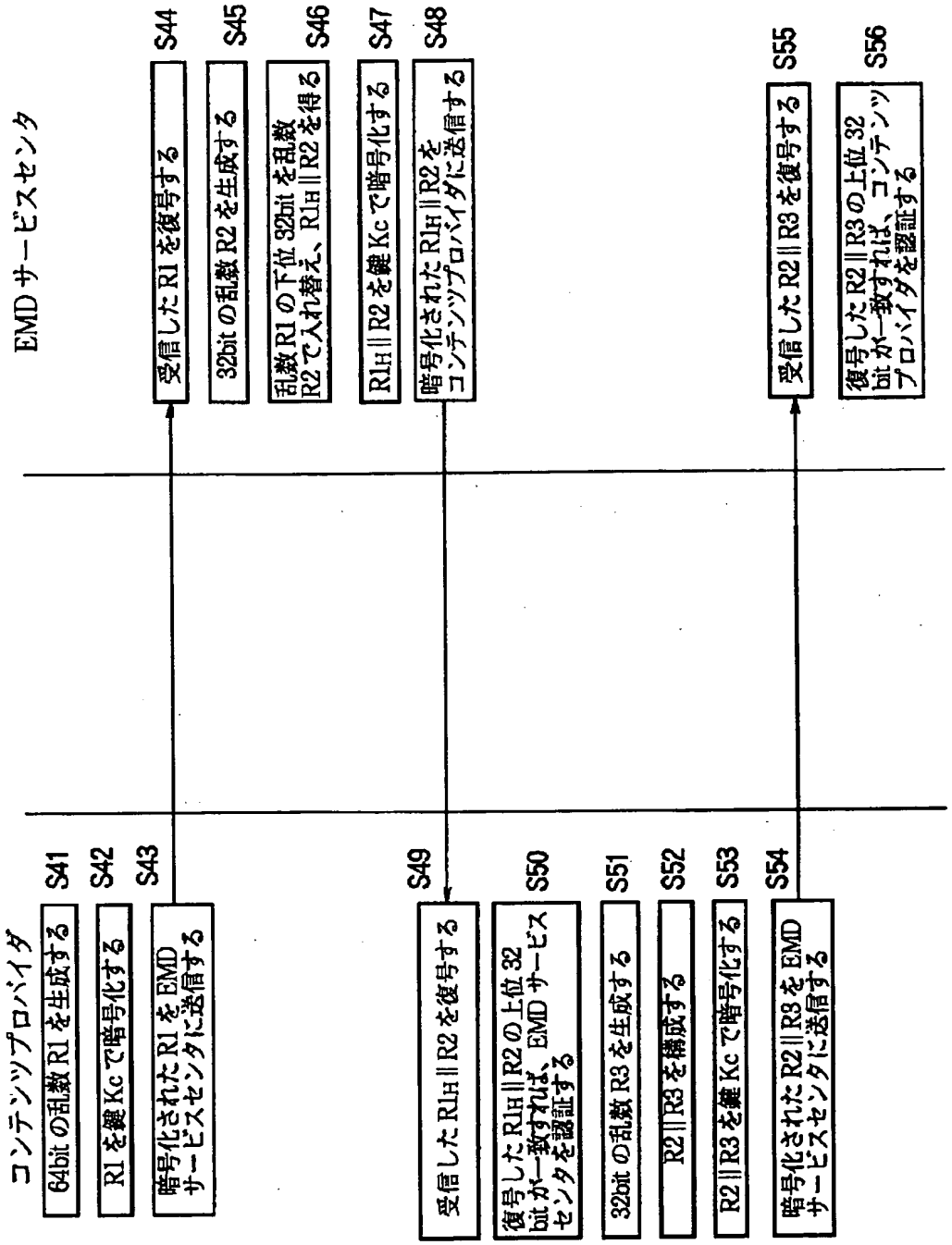
【図３４】


コンテンツ配布処理スタート
EMDサービスセンタは，コンテンツプロバイダに配送用鍵を送信し、コンテンツプロバイダは、配送用鍵を受信する
S11
ユーザは，機器情報をEMDサービスセンタに登録する
S12
EMDサービスセンタは、ユーザに配送用鍵を送信し、ユーザは配送用鍵を受信する
S13
コンテンツプロバイダは、サービスプロバイダにセキュアコンテナを送信し、サービスプロバイダはセキュアコンテナを受信する
S14
サービスプロバイダは、ユーザにセキュアコンテナを送信し、ユーザはセキュアコンテナを受信する
S15
ユーザは、課金処理を実行する
S16
ユーザは、コンテンツを再生する
S17
エンド

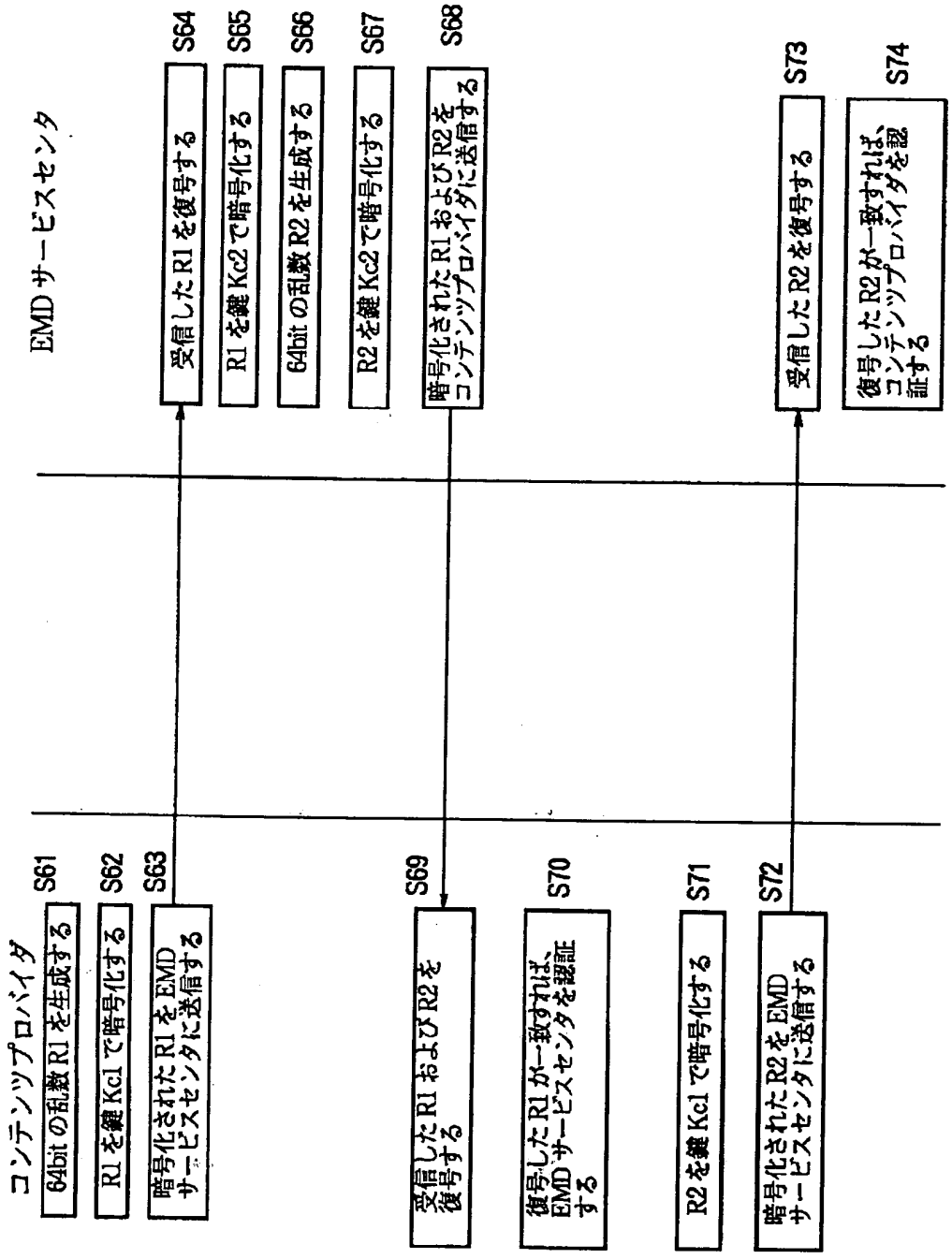
【図３５】


コンテンツ配布処理スタート
EMD サービスセンタは，コンテンツプロバイダに配送用鍵を送信し、コンテンツプロバイダは配送鍵を受信する
S21
EMD サービスセンタは，サービスプロバイダに配送用鍵を送信し、サービスプロバイダは配送鍵を受信する
S22
ユーザは，機器情報を EMD サービスセンタに登録する
S23
EMD サービスセンタは、ユーザに配送用鍵を送信し、ユーザは配送用鍵を受信する
S24
コンテンツプロバイダは、サービスプロバイダにセキュアコンテナを送信し、サービスプロバイダはセキュアコンテナを受信する
S25
サービスプロバイダは、ユーザにセキュアコンテナを送信し、ユーザはセキュアコンテナを受信する
S26
ユーザは、課金処理を実行する
S27
ユーザは、コンテンツを再生する
S28
エンド

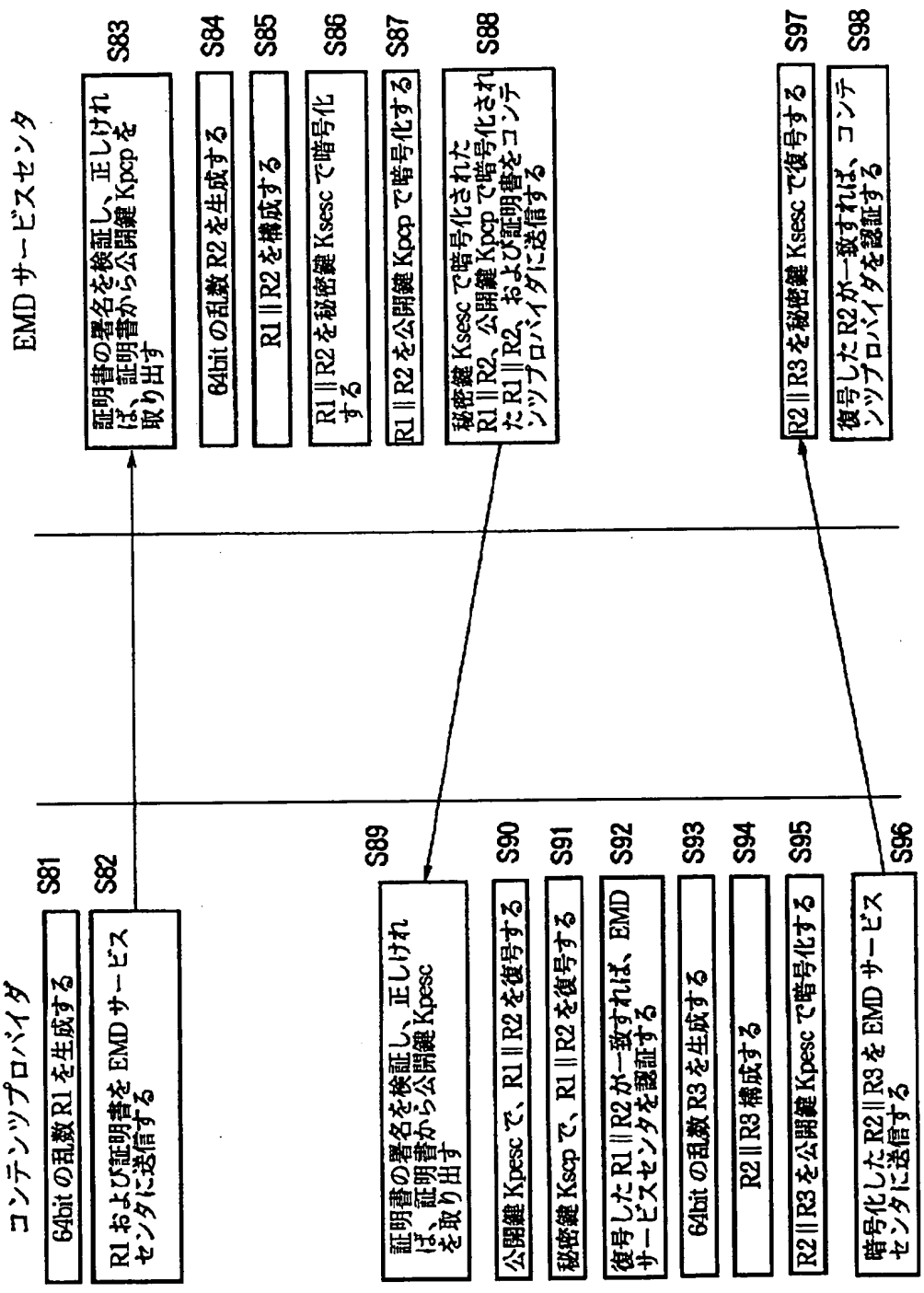
【図３７】


コンテンツプロバイダ
EMD サービスセンタ
S41
64bit の乱数 R1 を生成する
S42
R1 を鍵 Kc で暗号化する
S43
暗号化された R1 を EMD サービスセンタに送信する
S44
受信した R1 を復号する
S45
32bit の乱数 R2 を生成する
S46
乱数 R1 の下位 32bit を乱数 R2 で入れ替え、R1H||R2 を得る
S47
R1H||R2 を鍵 Kc で暗号化する
S48
暗号化された R1H||R2 をコンテンツプロバイダに送信する
S49
受信した R1H||R2 を復号する
S50
復号した R1H||R2 の上位 32bit が一致すれば、EMD サービスセンタを認証する
S51
32bit の乱数 R3 を生成する
S52
R2||R3 を構成する
S53
R2||R3 を鍵 Kc で暗号化する
S54
暗号化された R2||R3 を EMD サービスセンタに送信する
S55
受信した R2||R3 を復号する
S56
復号した R2||R3 の上位 32bit が一致すれば、コンテンツプロバイダを認証する

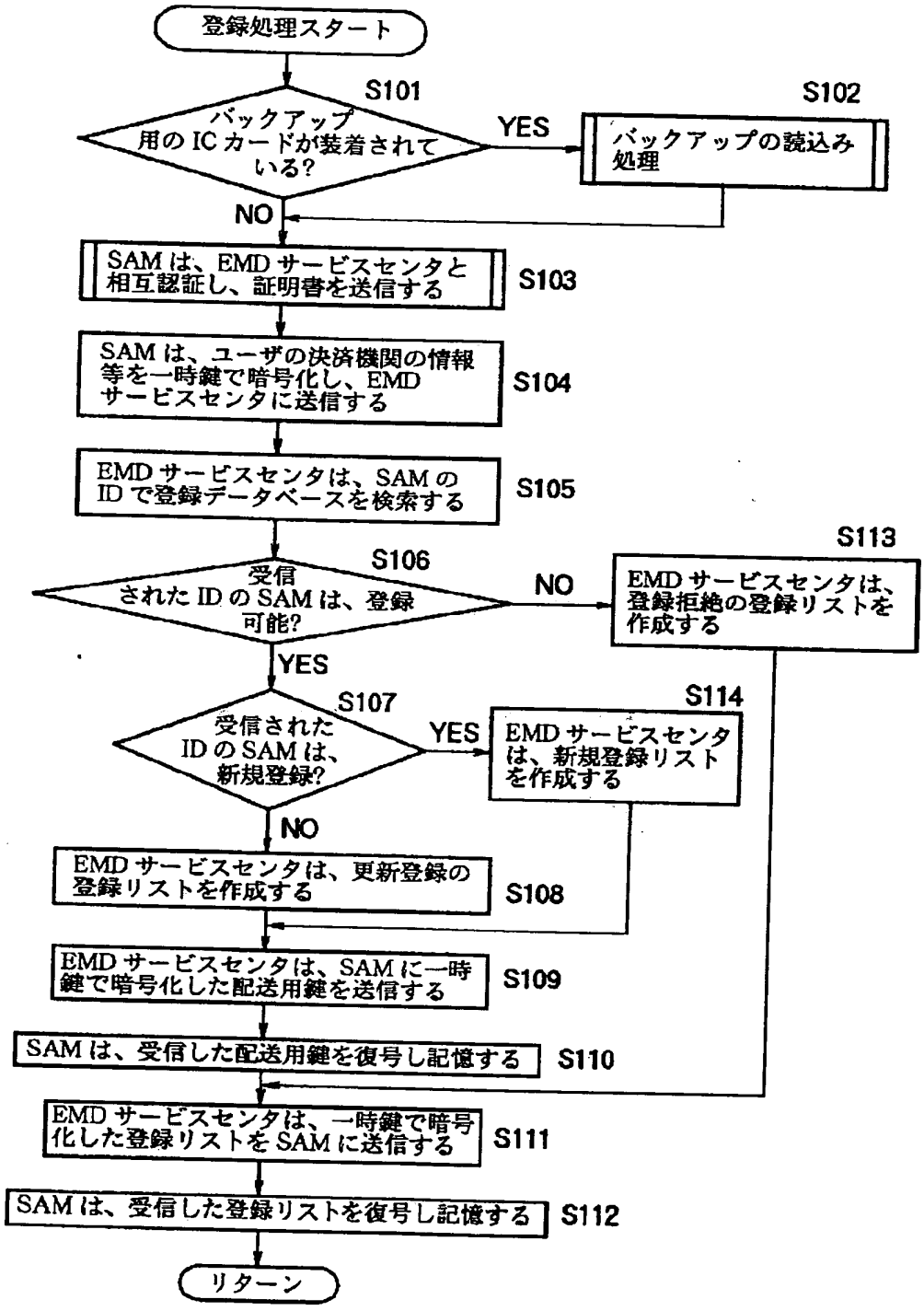
【図３８】


コンテンツプロバイダ
EMD サービスセンタ
S61
64bit の乱数 R1 を生成する
S62
R1 を鍵 Kc1 で暗号化する
S63
暗号化された R1 を EMD サービスセンタに送信する
S64
受信した R1 を復号する
S65
R1 を鍵 Kc2 で暗号化する
S66
64bit の乱数 R2 を生成する
S67
R2 を鍵 Kc2 で暗号化する
S68
暗号化された R1 および R2 をコンテンツプロバイダに送信する
S69
受信した R1 および R2 を復号する
S70
復号した R1 が一致すれば、EMD サービスセンタを認証する
S71
R2 を鍵 Kc1 で暗号化する
S72
暗号化された R2 を EMD サービスセンタに送信する
S73
受信した R2 を復号する
S74
復号した R2 が一致すれば、コンテンツプロバイダを認証する

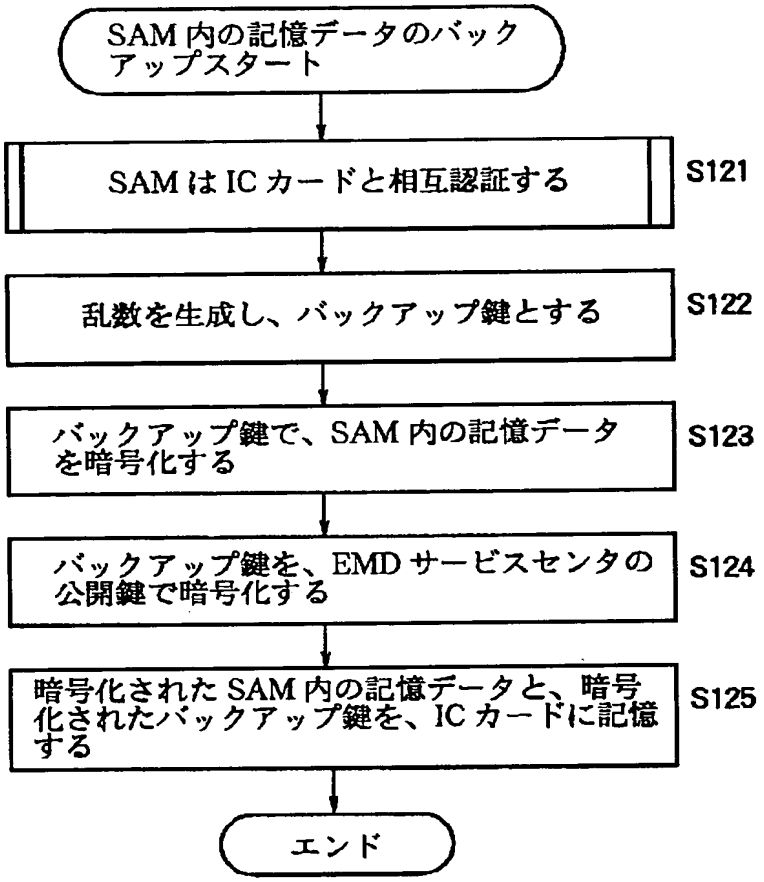
【図３９】


EMD サービスセンタ
コンテンツプロバイダ
S81
64bit の乱数 R1 を生成する
S82
R1 および証明書を EMD サービスセンタに送信する
S83
証明書の署名を検証し、正しければ、証明書から公開鍵 Kpcp を取り出す
S84
64bit の乱数 R2 を生成する
S85
R1 ‖ R2 を構成する
S86
R1 ‖ R2 を秘密鍵 Ksesc で暗号化する
S87
R1 ‖ R2 を公開鍵 Kpcp で暗号化する
S88
秘密鍵 Ksesc で暗号化された R1 ‖ R2、公開鍵 Kpcp で暗号化された R1 ‖ R2、および証明書をコンテンツプロバイダに送信する
S89
証明書の署名を検証し、正しければ、証明書から公開鍵 Kpesc を取り出す
S90
公開鍵 Kpesc で、R1 ‖ R2 を復号する
S91
秘密鍵 Kscp で、R1 ‖ R2 を復号する
S92
復号した R1 ‖ R2 が一致すれば、EMD サービスセンタを認証する
S93
64bit の乱数 R3 を生成する
S94
R2 ‖ R3 を構成する
S95
R2 ‖ R3 を公開鍵 Kpesc で暗号化する
S96
暗号化した R2 ‖ R3 を EMD サービスセンタに送信する
S97
R2 ‖ R3 を秘密鍵 Ksesc で復号する
S98
復号した R2 が一致すれば、コンテンツプロバイダを認証する

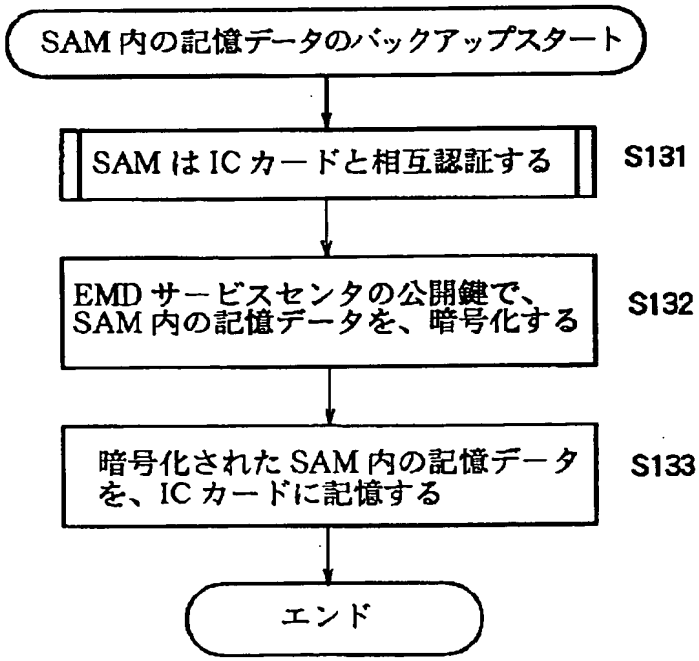
【図４０】


登録処理スタート
S101
バックアップ用のICカードが装着されている?
YES
S102
バックアップの読込み処理
NO
SAMは、EMDサービスセンタと相互認証し、証明書を送信する
S103
SAMは、ユーザの決済機関の情報等を一時鍵で暗号化し、EMDサービスセンタに送信する
S104
EMDサービスセンタは、SAMのIDで登録データベースを検索する
S105
S106
受信されたIDのSAMは、登録可能?
NO
S113
EMDサービスセンタは、登録拒絶の登録リストを作成する
YES
S107
受信されたIDのSAMは、新規登録?
YES
S114
EMDサービスセンタは、新規登録リストを作成する
NO
EMDサービスセンタは、更新登録の登録リストを作成する
S108
EMDサービスセンタは、SAMに一時鍵で暗号化した配送用鍵を送信する
S109
SAMは、受信した配送用鍵を復号し記憶する
S110
EMDサービスセンタは、一時鍵で暗号化した登録リストをSAMに送信する
S111
SAMは、受信した登録リストを復号し記憶する
S112
リターン

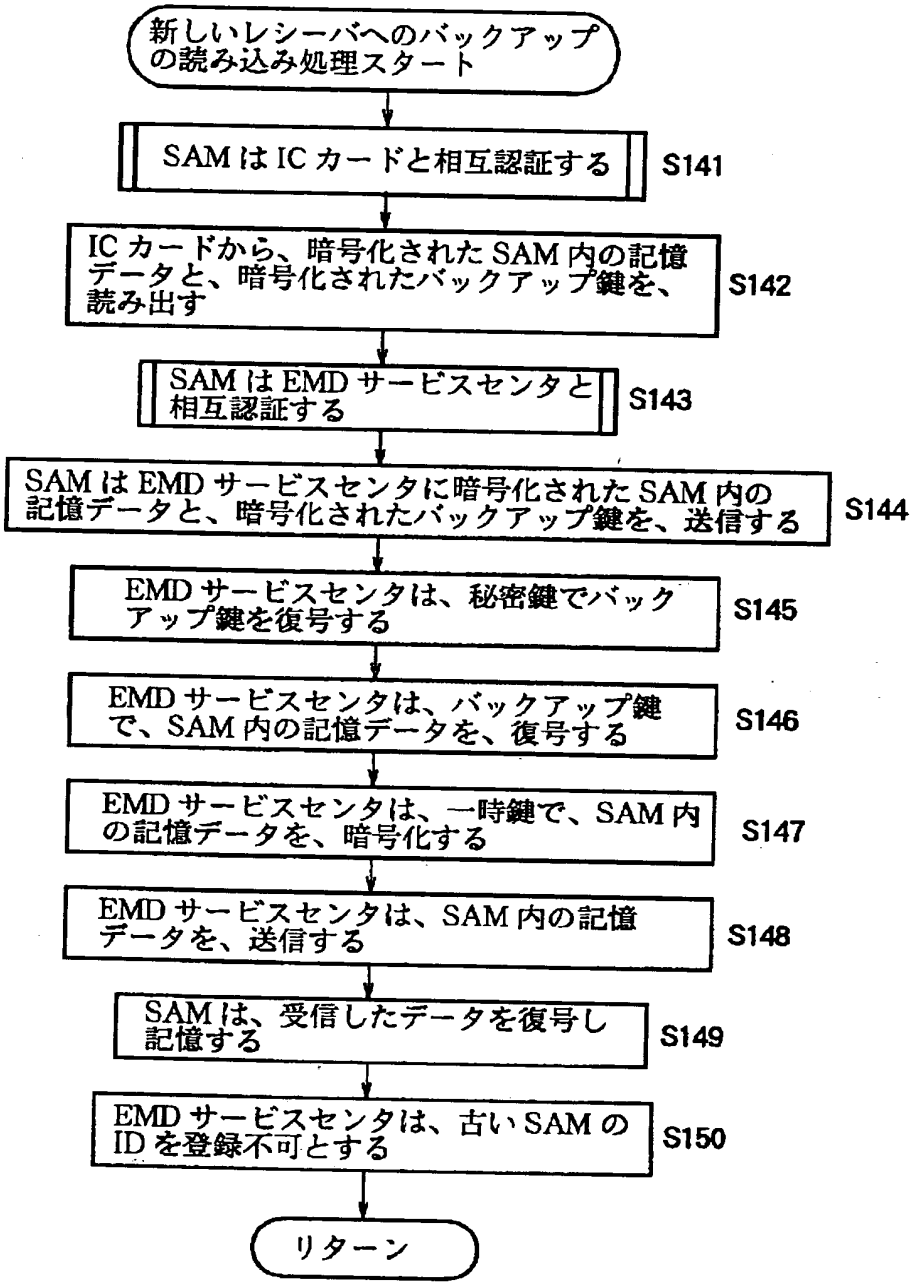
【図４３】


SAM 内の記憶データのバックアップスタート
SAM は IC カードと相互認証する
S121
乱数を生成し、バックアップ鍵とする
S122
バックアップ鍵で、SAM 内の記憶データを暗号化する
S123
バックアップ鍵を、EMD サービスセンタの公開鍵で暗号化する
S124
暗号化された SAM 内の記憶データと、暗号化されたバックアップ鍵を、IC カードに記憶する
S125
エンド

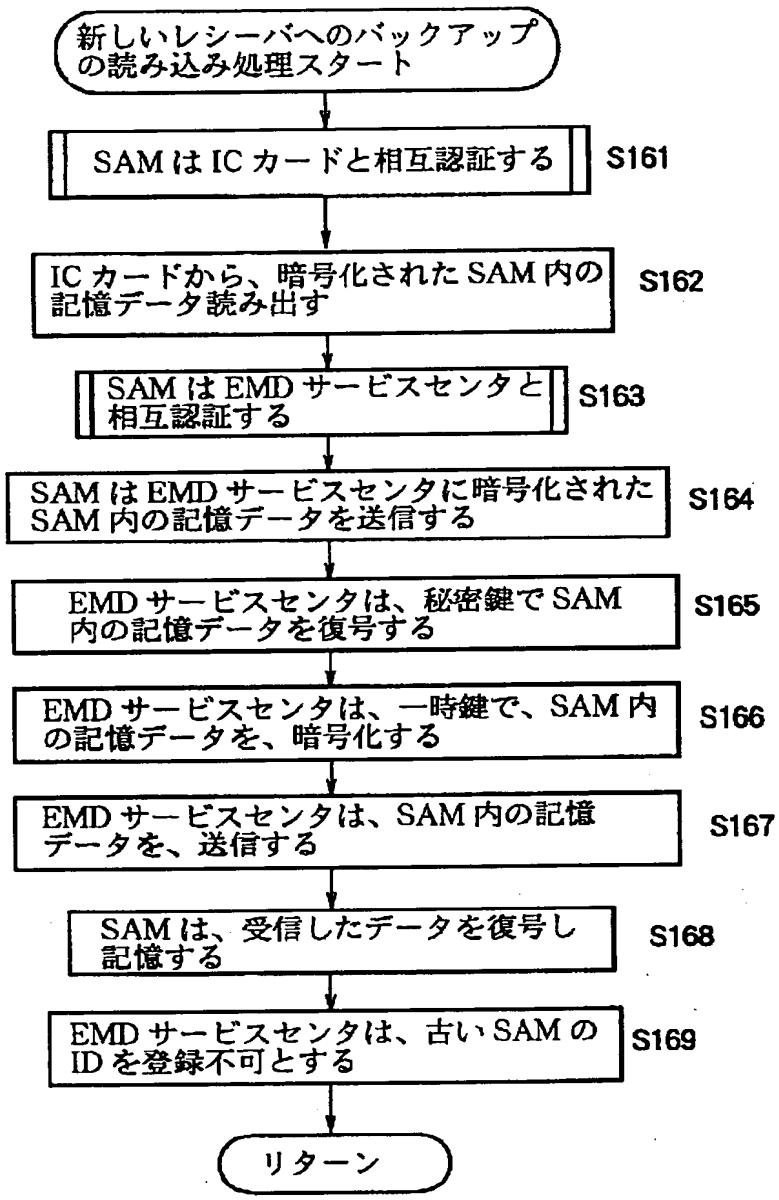
【図４４】


SAM 内の記憶データのバックアップスタート
SAM は IC カードと相互認証する
S131
EMD サービスセンタの公開鍵で、SAM 内の記憶データを、暗号化する
S132
暗号化された SAM 内の記憶データを、IC カードに記憶する
S133
エンド

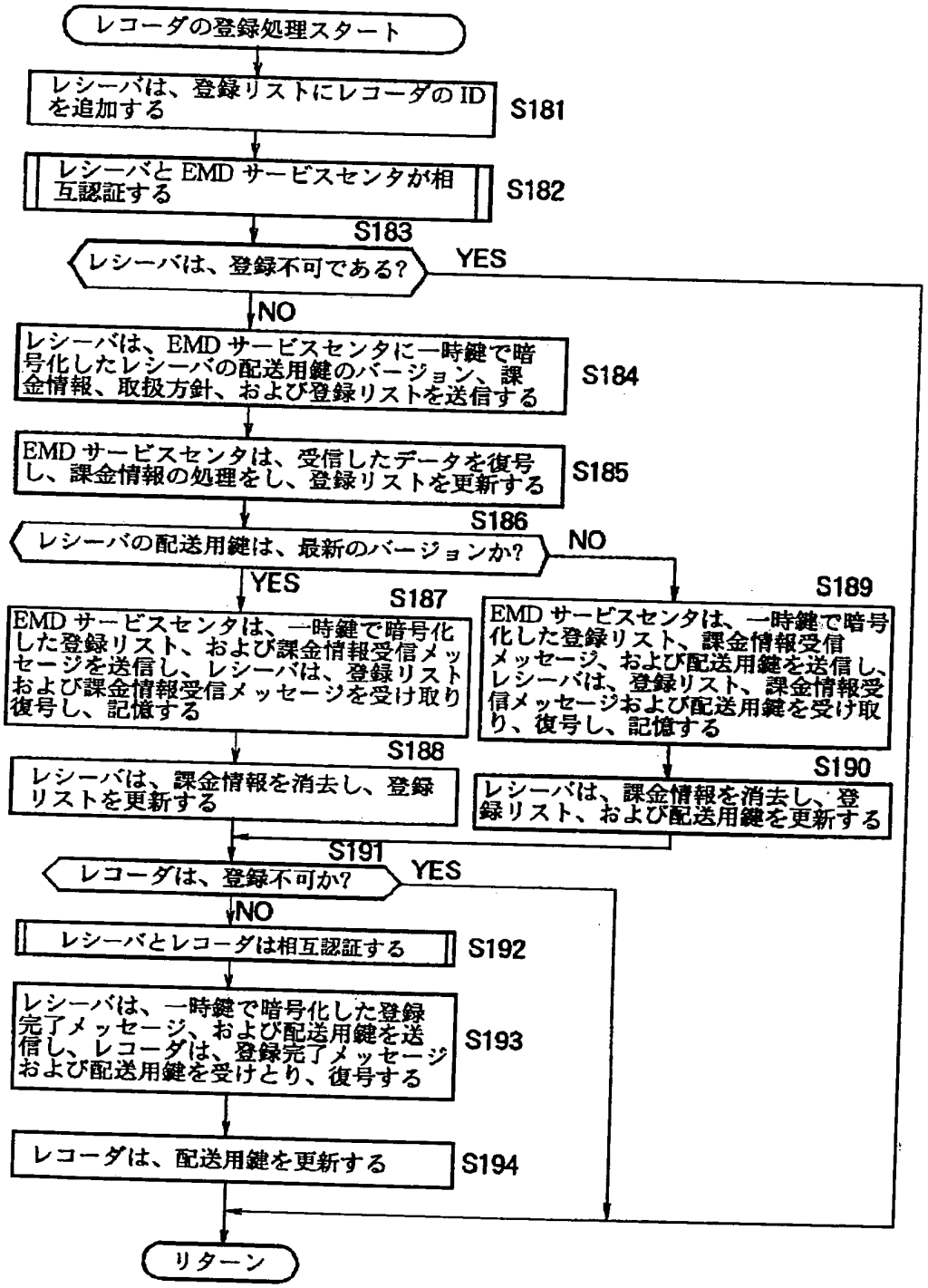
【図４５】


新しいレシーバへのバックアップの読み込み処理スタート
SAMはICカードと相互認証する
S141
ICカードから、暗号化されたSAM内の記憶データと、暗号化されたバックアップ鍵を、読み出す
S142
SAMはEMDサービスセンタと相互認証する
S143
SAMはEMDサービスセンタに暗号化されたSAM内の記憶データと、暗号化されたバックアップ鍵を、送信する
S144
EMDサービスセンタは、秘密鍵でバックアップ鍵を復号する
S145
EMDサービスセンタは、バックアップ鍵で、SAM内の記憶データを、復号する
S146
EMDサービスセンタは、一時鍵で、SAM内の記憶データを、暗号化する
S147
EMDサービスセンタは、SAM内の記憶データを、送信する
S148
SAMは、受信したデータを復号し記憶する
S149
EMDサービスセンタは、古いSAMのIDを登録不可とする
S150
リターン

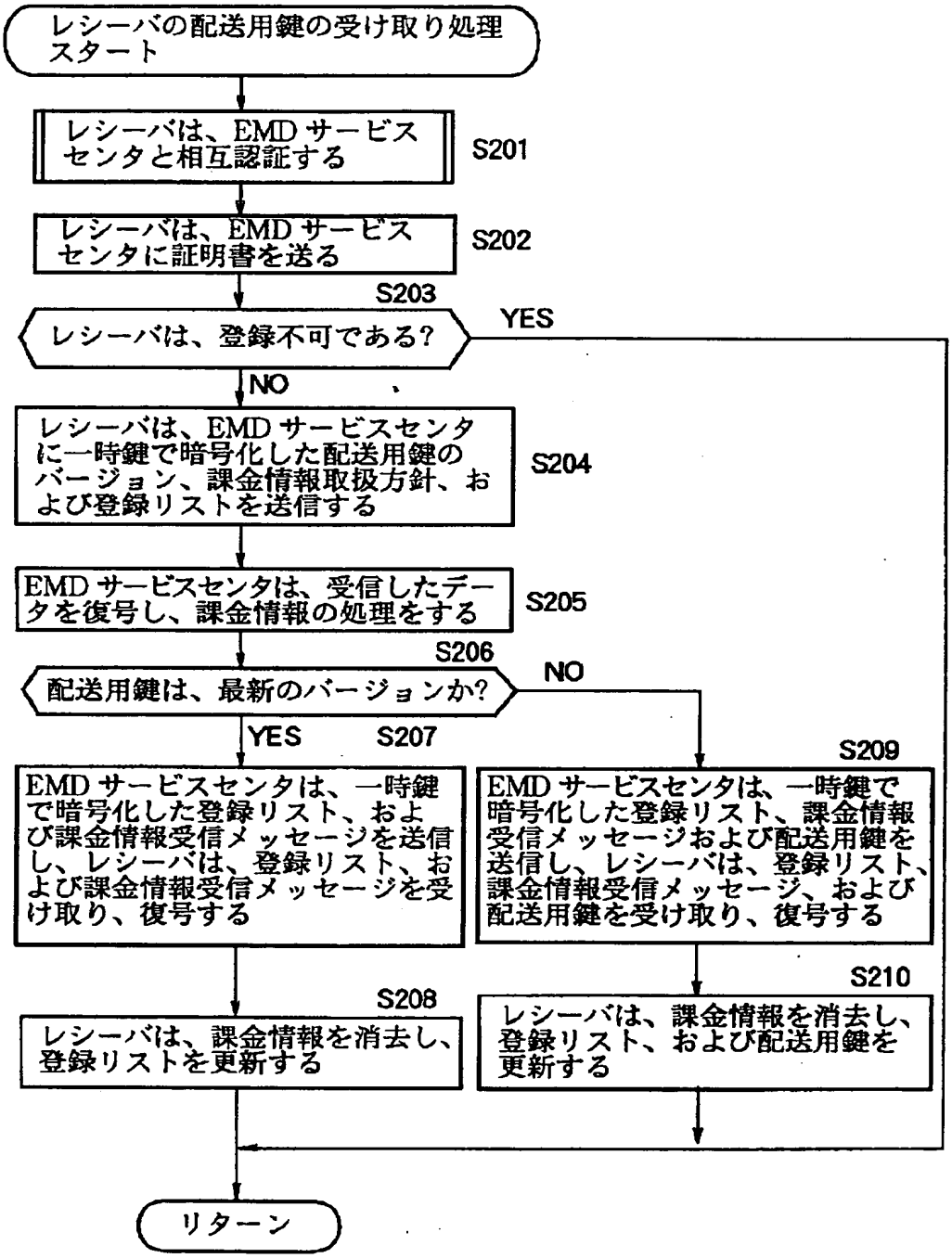
【図４６】


新しいレシーバへのバックアップの読み込み処理スタート
SAMはICカードと相互認証する
S161
ICカードから、暗号化されたSAM内の記憶データ読み出す
S162
SAMはEMDサービスセンタと相互認証する
S163
SAMはEMDサービスセンタに暗号化されたSAM内の記憶データを送信する
S164
EMDサービスセンタは、秘密鍵でSAM内の記憶データを復号する
S165
EMDサービスセンタは、一時鍵で、SAM内の記憶データを、暗号化する
S166
EMDサービスセンタは、SAM内の記憶データを、送信する
S167
SAMは、受信したデータを復号し記憶する
S168
EMDサービスセンタは、古いSAMのIDを登録不可とする
S169
リターン

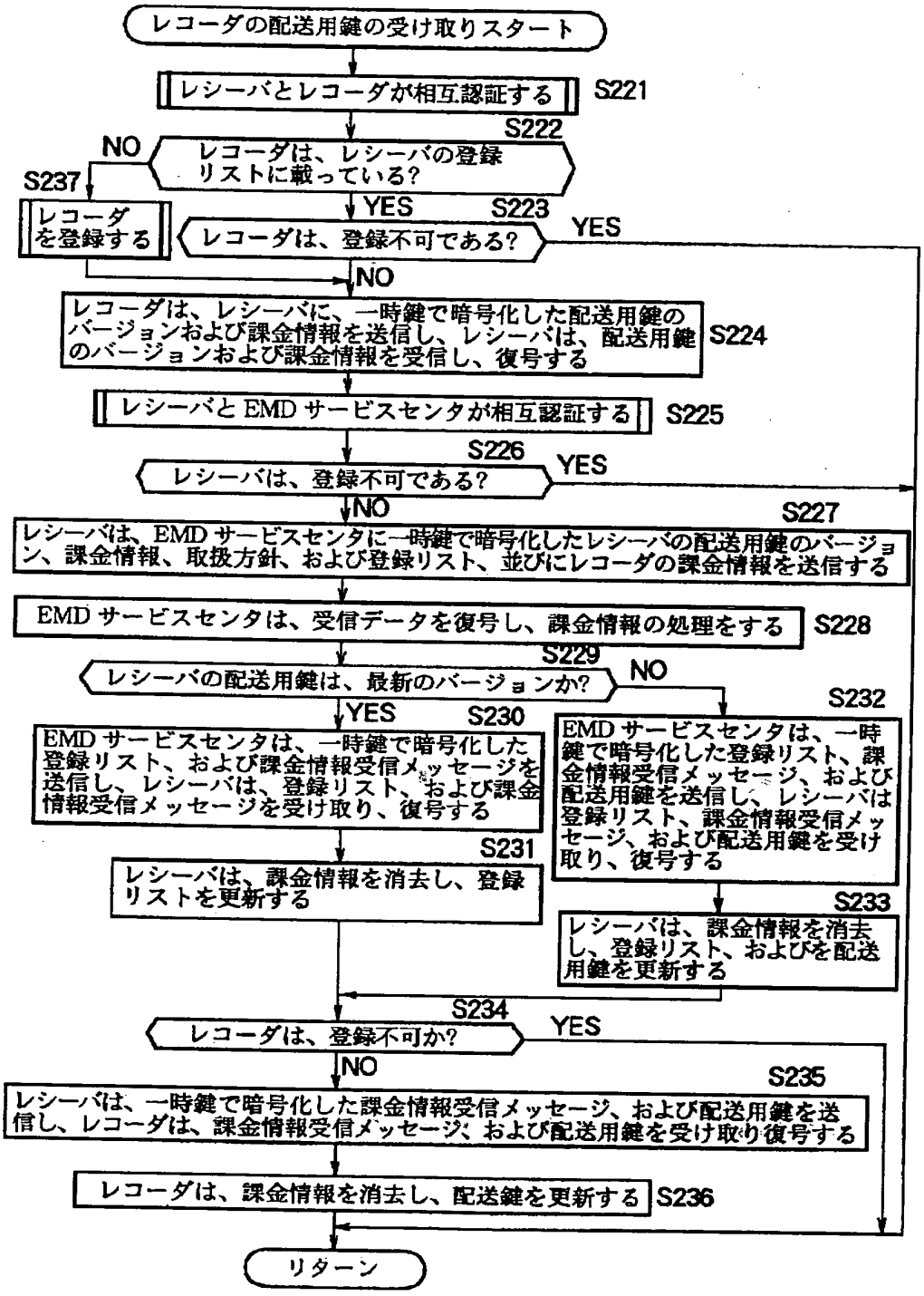
【図４７】


レコーダの登録処理スタート
レシーバは、登録リストにレコーダのIDを追加する
S181
レシーバとEMDサービスセンタが相互認証する
S182
S183
レシーバは、登録不可である?
YES
NO
レシーバは、EMDサービスセンタに一時鍵で暗号化したレシーバの配送用鍵のバージョン、課金情報、取扱方針、および登録リストを送信する
S184
EMDサービスセンタは、受信したデータを復号し、課金情報の処理をし、登録リストを更新する
S185
S186
レシーバの配送用鍵は、最新のバージョンか?
NO
YES
S187
EMDサービスセンタは、一時鍵で暗号化した登録リスト、および課金情報受信メッセージを送信し、レシーバは、登録リストおよび課金情報受信メッセージを受け取り復号し、記憶する
S189
EMDサービスセンタは、一時鍵で暗号化した登録リスト、課金情報受信メッセージ、および配送用鍵を送信し、レシーバは、登録リスト、課金情報受信メッセージおよび配送用鍵を受け取り、復号し、記憶する
S188
レシーバは、課金情報を消去し、登録リストを更新する
S190
レシーバは、課金情報を消去し、登録リスト、および配送用鍵を更新する
S191
レコーダは、登録不可か?
YES
NO
レシーバとレコーダは相互認証する
S192
レシーバは、一時鍵で暗号化した登録完了メッセージ、および配送用鍵を送信し、レコーダは、登録完了メッセージおよび配送用鍵を受けとり、復号する
S193
レコーダは、配送用鍵を更新する
S194
リターン

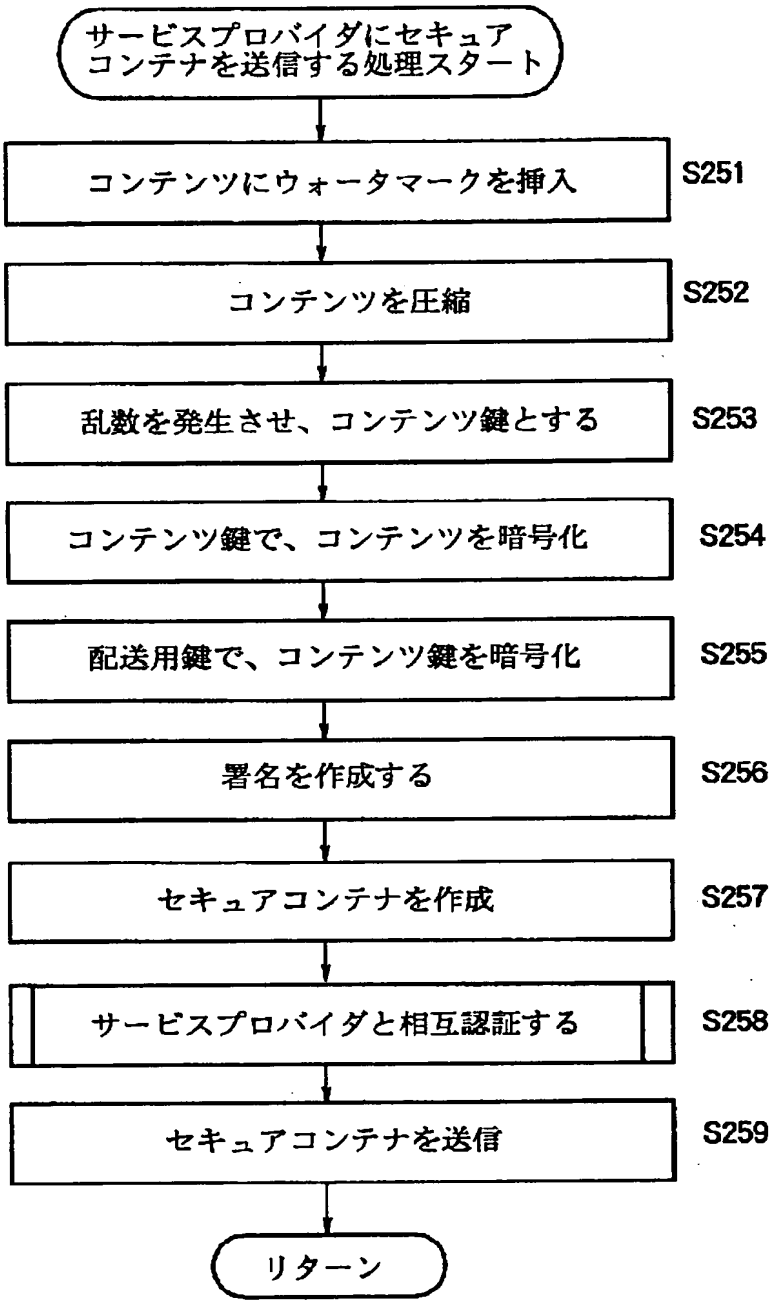
【図４８】


レシーバの配送用鍵の受け取り処理スタート
レシーバは、EMD サービスセンタと相互認証する
S201
レシーバは、EMD サービスセンタに証明書を送る
S202
S203
レシーバは、登録不可である?
YES
NO
レシーバは、EMD サービスセンタに一時鍵で暗号化した配送用鍵のバージョン、課金情報取扱方針、および登録リストを送信する
S204
EMD サービスセンタは、受信したデータを復号し、課金情報の処理をする
S205
S206
配送用鍵は、最新のバージョンか?
NO
YES
S207
EMD サービスセンタは、一時鍵で暗号化した登録リスト、および課金情報受信メッセージを送信し、レシーバは、登録リスト、および課金情報受信メッセージを受け取り、復号する
S209
EMD サービスセンタは、一時鍵で暗号化した登録リスト、課金情報受信メッセージおよび配送用鍵を送信し、レシーバは、登録リスト、課金情報受信メッセージ、および配送用鍵を受け取り、復号する
S208
レシーバは、課金情報を消去し、登録リストを更新する
S210
レシーバは、課金情報を消去し、登録リスト、および配送用鍵を更新する
リターン

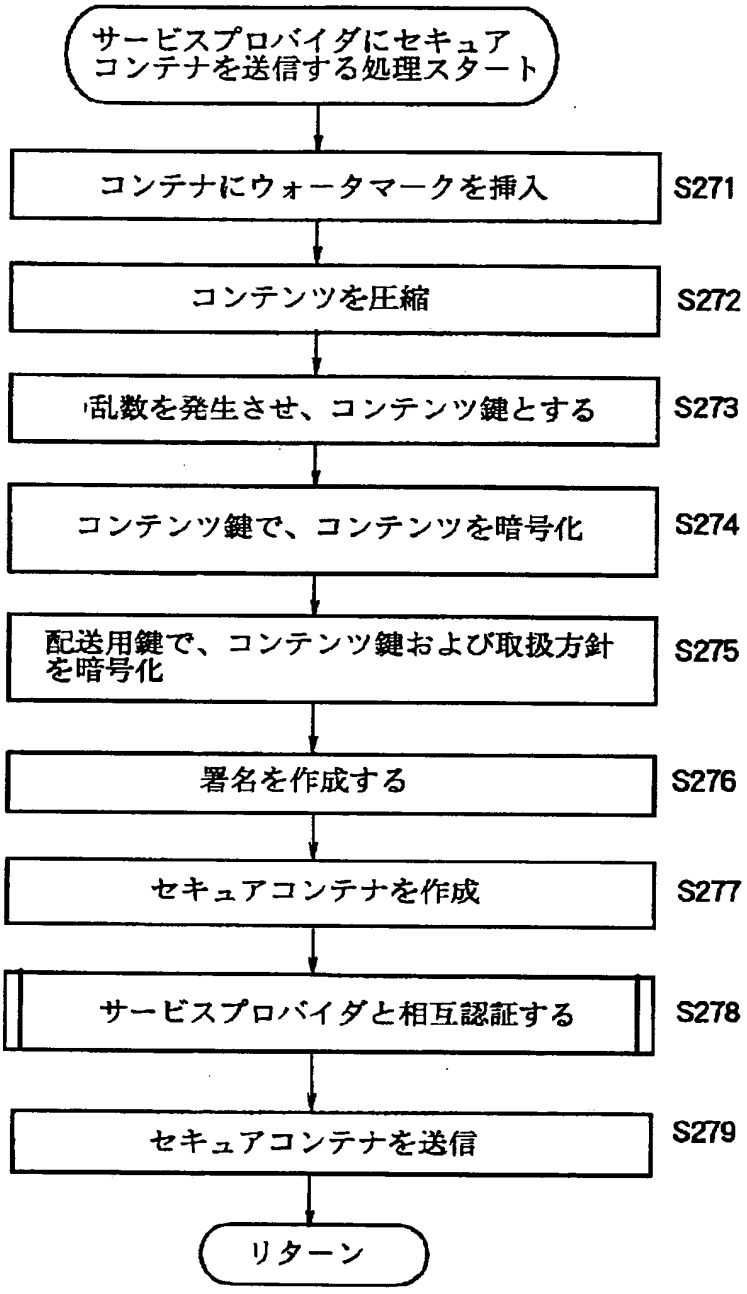
【図４９】


レコーダの配送用鍵の受け取りスタート
レシーバとレコーダが相互認証する
S221
S222
NO
レコーダは、レシーバの登録リストに載っている?
S237
レコーダを登録する
YES
S223
レコーダは、登録不可である?
YES
NO
レコーダは、レシーバに、一時鍵で暗号化した配送用鍵のバージョンおよび課金情報を送信し、レシーバは、配送用鍵のバージョンおよび課金情報を受信し、復号する
S224
レシーバとEMDサービスセンタが相互認証する
S225
S226
レシーバは、登録不可である?
YES
NO
S227
レシーバは、EMDサービスセンタに一時鍵で暗号化したレシーバの配送用鍵のバージョン、課金情報、取扱方針、および登録リスト、並びにレコーダの課金情報を送信する
EMDサービスセンタは、受信データを復号し、課金情報の処理をする
S228
S229
レシーバの配送用鍵は、最新のバージョンか?
NO
S232
YES
S230
EMDサービスセンタは、一時鍵で暗号化した登録リスト、および課金情報受信メッセージを送信し、レシーバは、登録リスト、および課金情報受信メッセージを受け取り、復号する
EMDサービスセンタは、一時鍵で暗号化した登録リスト、課金情報受信メッセージ、および配送用鍵を送信し、レシーバは登録リスト、課金情報受信メッセージ、および配送用鍵を受け取り、復号する
S231
レシーバは、課金情報を消去し、登録リストを更新する
S233
レシーバは、課金情報を消去し、登録リスト、およびを配送用鍵を更新する
S234
レコーダは、登録不可か?
YES
NO
S235
レシーバは、一時鍵で暗号化した課金情報受信メッセージ、および配送用鍵を送信し、レコーダは、課金情報受信メッセージ、および配送用鍵を受け取り復号する
レコーダは、課金情報を消去し、配送鍵を更新する
S236
リターン

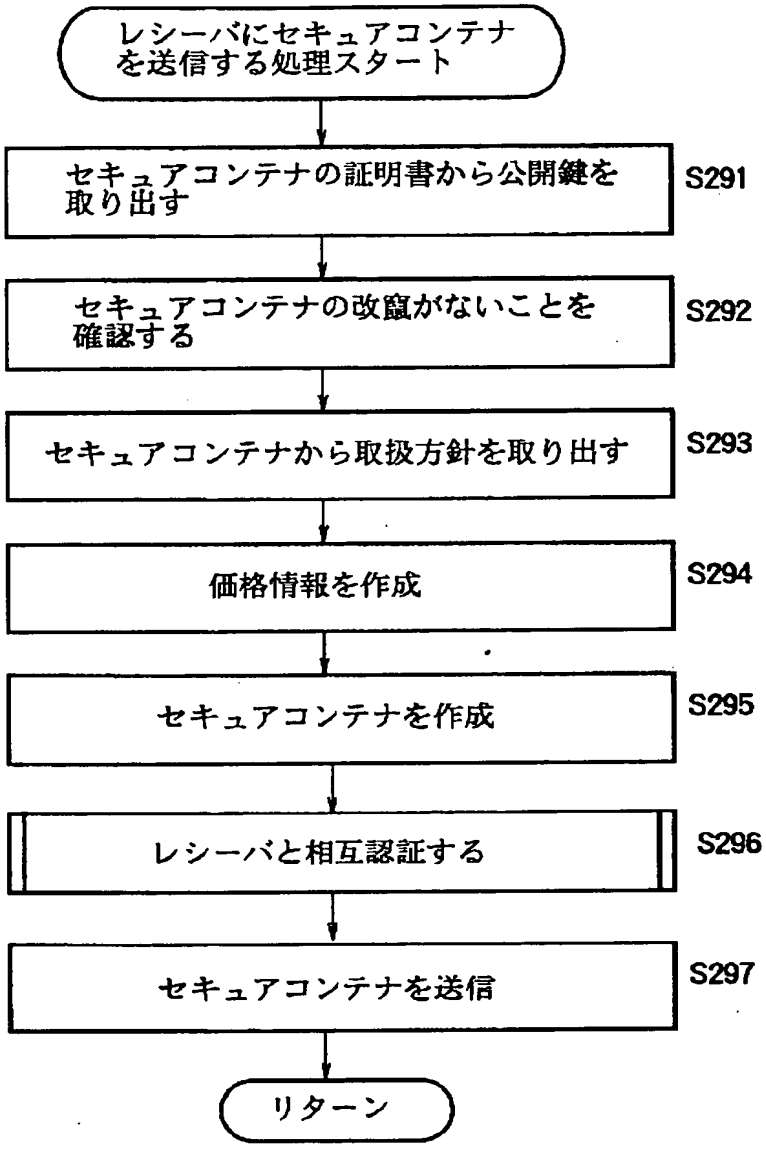
【図５０】


サービスプロバイダにセキュアコンテナを送信する処理スタート
コンテンツにウォータマークを挿入
S251
コンテンツを圧縮
S252
乱数を発生させ、コンテンツ鍵とする
S253
コンテンツ鍵で、コンテンツを暗号化
S254
配送用鍵で、コンテンツ鍵を暗号化
S255
署名を作成する
S256
セキュアコンテナを作成
S257
サービスプロバイダと相互認証する
S258
セキュアコンテナを送信
S259
リターン

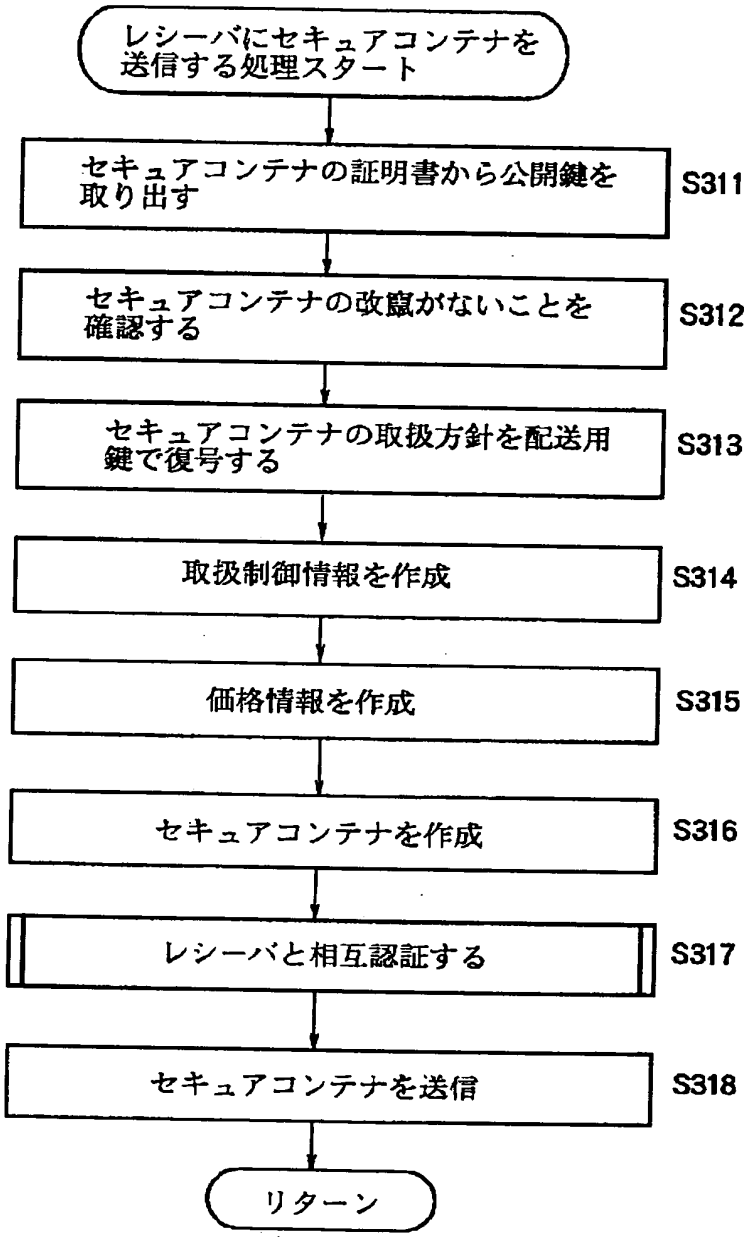
【図５１】


サービスプロバイダにセキュアコンテナを送信する処理スタート
コンテナにウォータマークを挿入
S271
コンテンツを圧縮
S272
乱数を発生させ、コンテンツ鍵とする
S273
コンテンツ鍵で、コンテンツを暗号化
S274
配送用鍵で、コンテンツ鍵および取扱方針を暗号化
S275
署名を作成する
S276
セキュアコンテナを作成
S277
サービスプロバイダと相互認証する
S278
セキュアコンテナを送信
S279
リターン

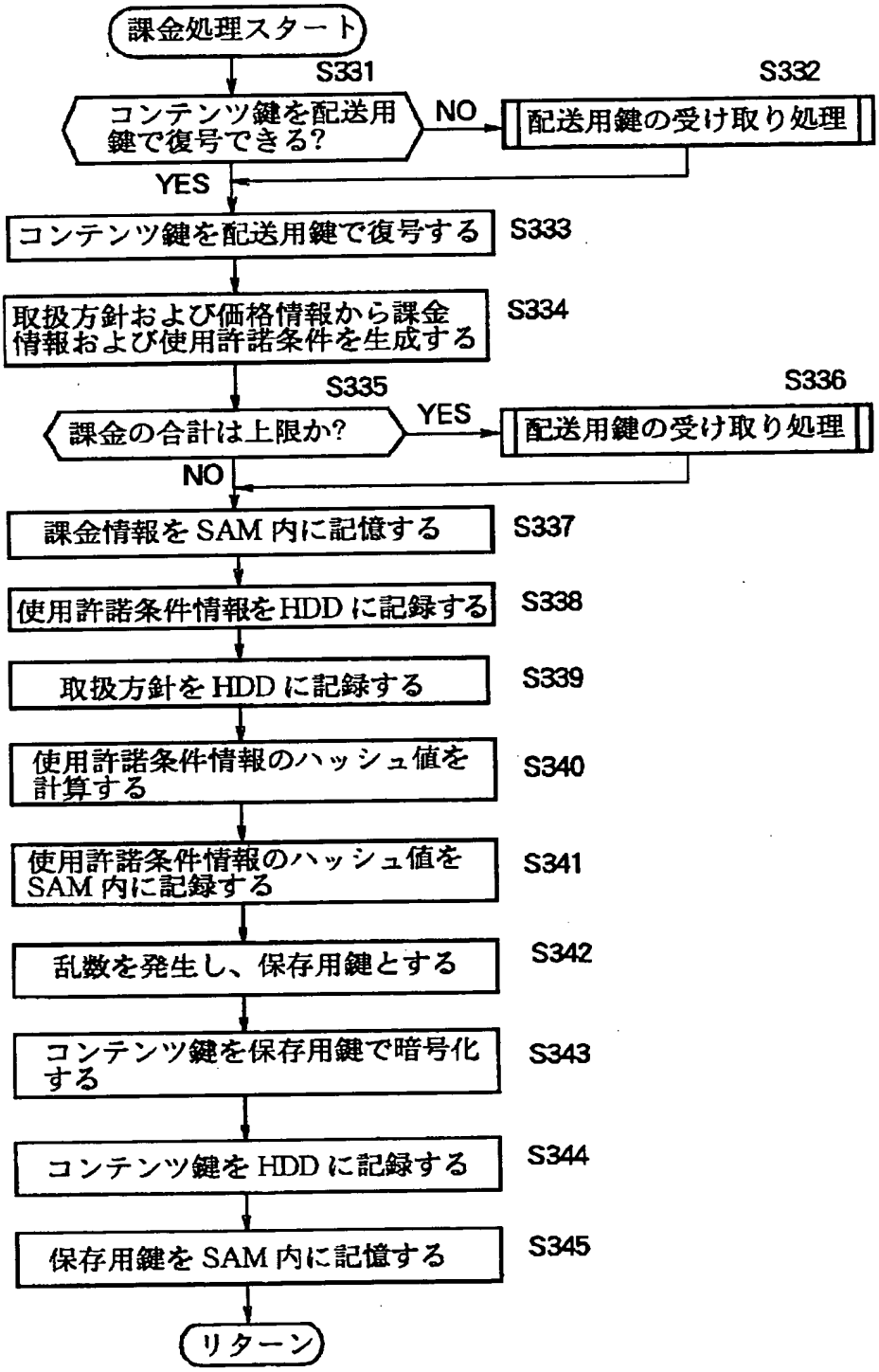
【図５２】


レシーバにセキュアコンテナを送信する処理スタート
セキュアコンテナの証明書から公開鍵を取り出す
S291
セキュアコンテナの改竄がないことを確認する
S292
セキュアコンテナから取扱方針を取り出す
S293
価格情報を作成
S294
セキュアコンテナを作成
S295
レシーバと相互認証する
S296
セキュアコンテナを送信
S297
リターン

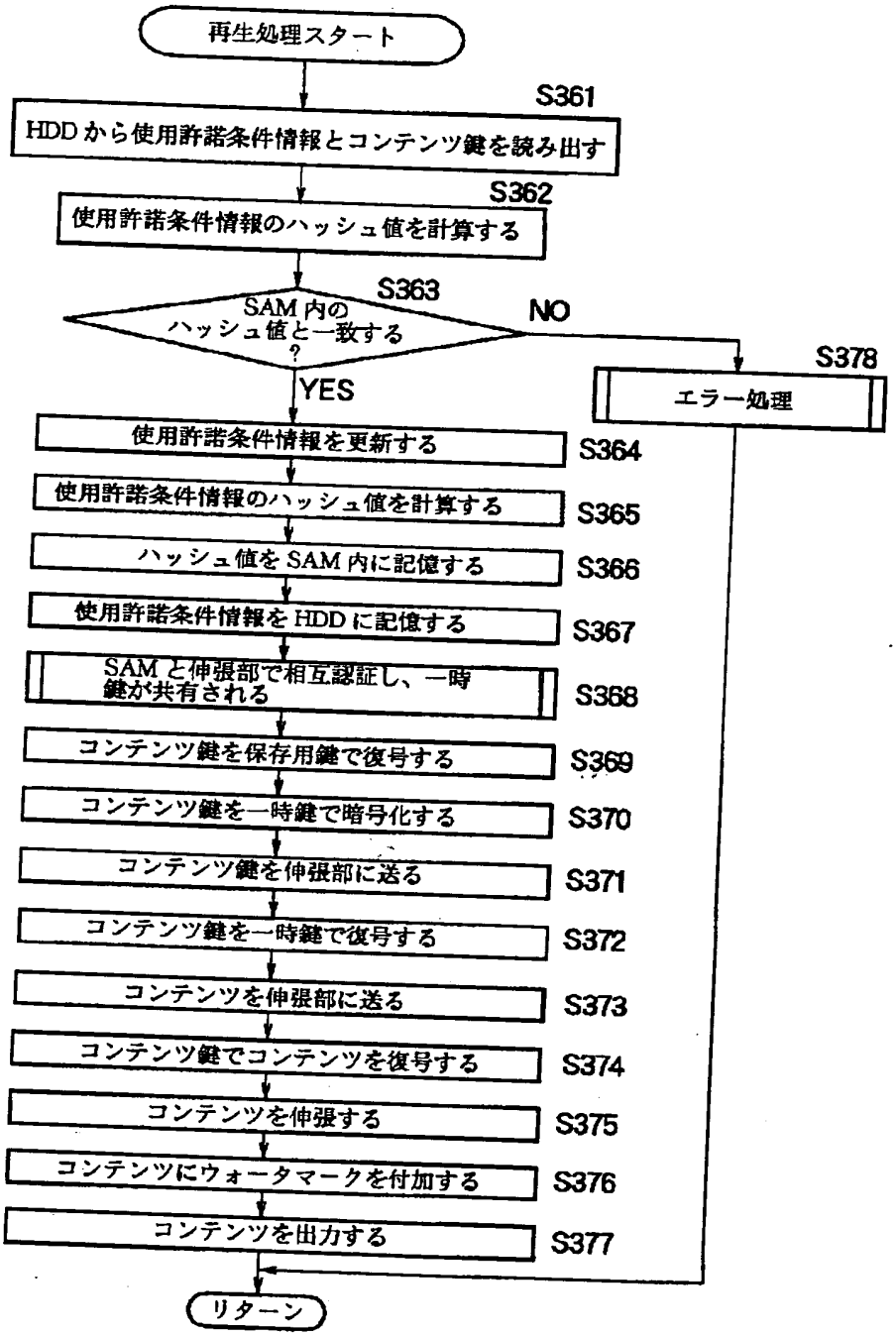
【図５３】


レシーバにセキュアコンテナを送信する処理スタート
セキュアコンテナの証明書から公開鍵を取り出す
S311
セキュアコンテナの改竄がないことを確認する
S312
セキュアコンテナの取扱方針を配送用鍵で復号する
S313
取扱制御情報を作成
S314
価格情報を作成
S315
セキュアコンテナを作成
S316
レシーバと相互認証する
S317
セキュアコンテナを送信
S318
リターン

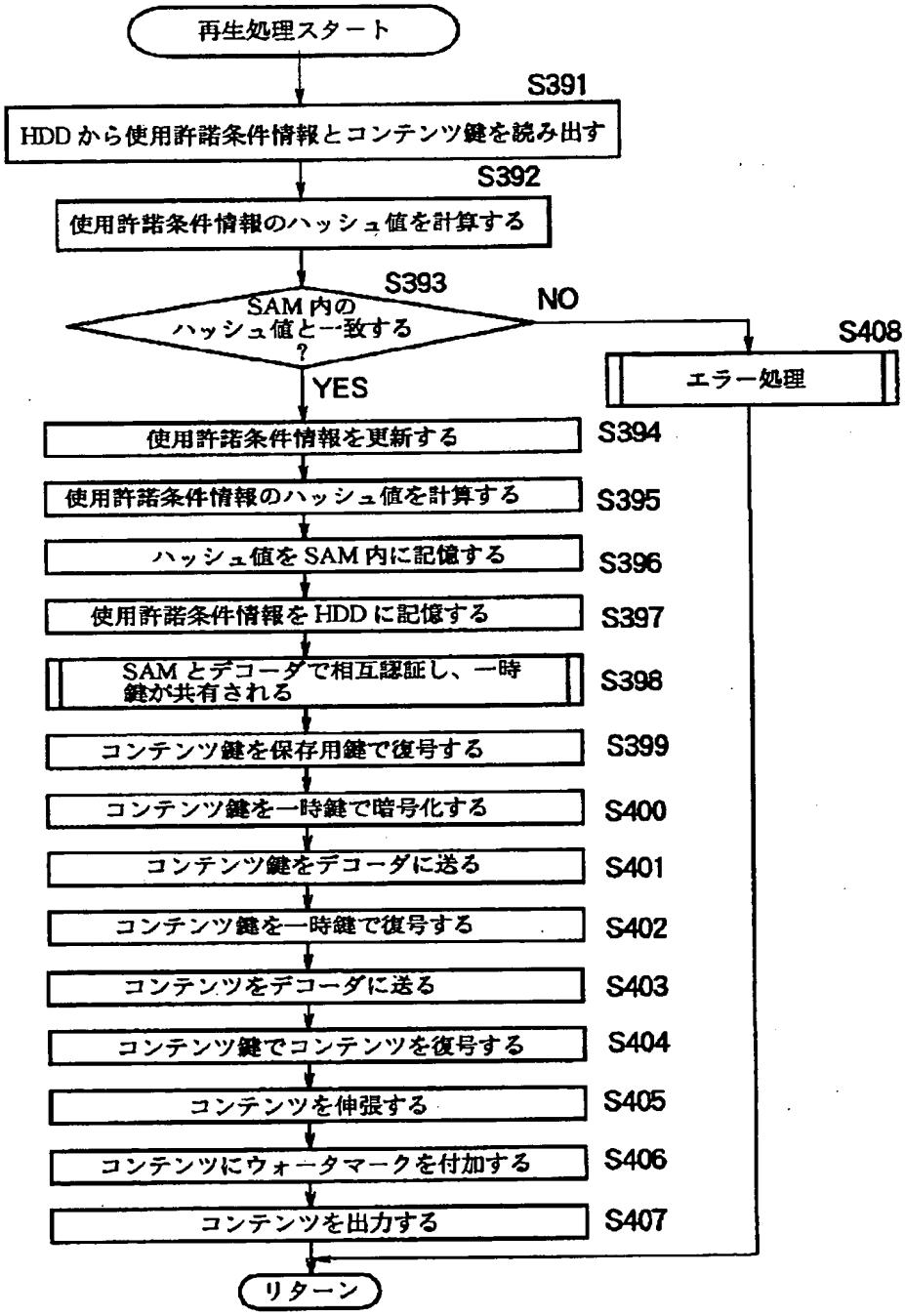
【図５４】


課金処理スタート
S331
コンテンツ鍵を配送用鍵で復号できる?
NO
S332
配送用鍵の受け取り処理
YES
コンテンツ鍵を配送用鍵で復号する
S333
取扱方針および価格情報から課金情報および使用許諾条件を生成する
S334
S335
課金の合計は上限か?
YES
S336
配送用鍵の受け取り処理
NO
課金情報をSAM内に記憶する
S337
使用許諾条件情報をHDDに記録する
S338
取扱方針をHDDに記録する
S339
使用許諾条件情報のハッシュ値を計算する
S340
使用許諾条件情報のハッシュ値をSAM内に記録する
S341
乱数を発生し、保存用鍵とする
S342
コンテンツ鍵を保存用鍵で暗号化する
S343
コンテンツ鍵をHDDに記録する
S344
保存用鍵をSAM内に記憶する
S345
リターン

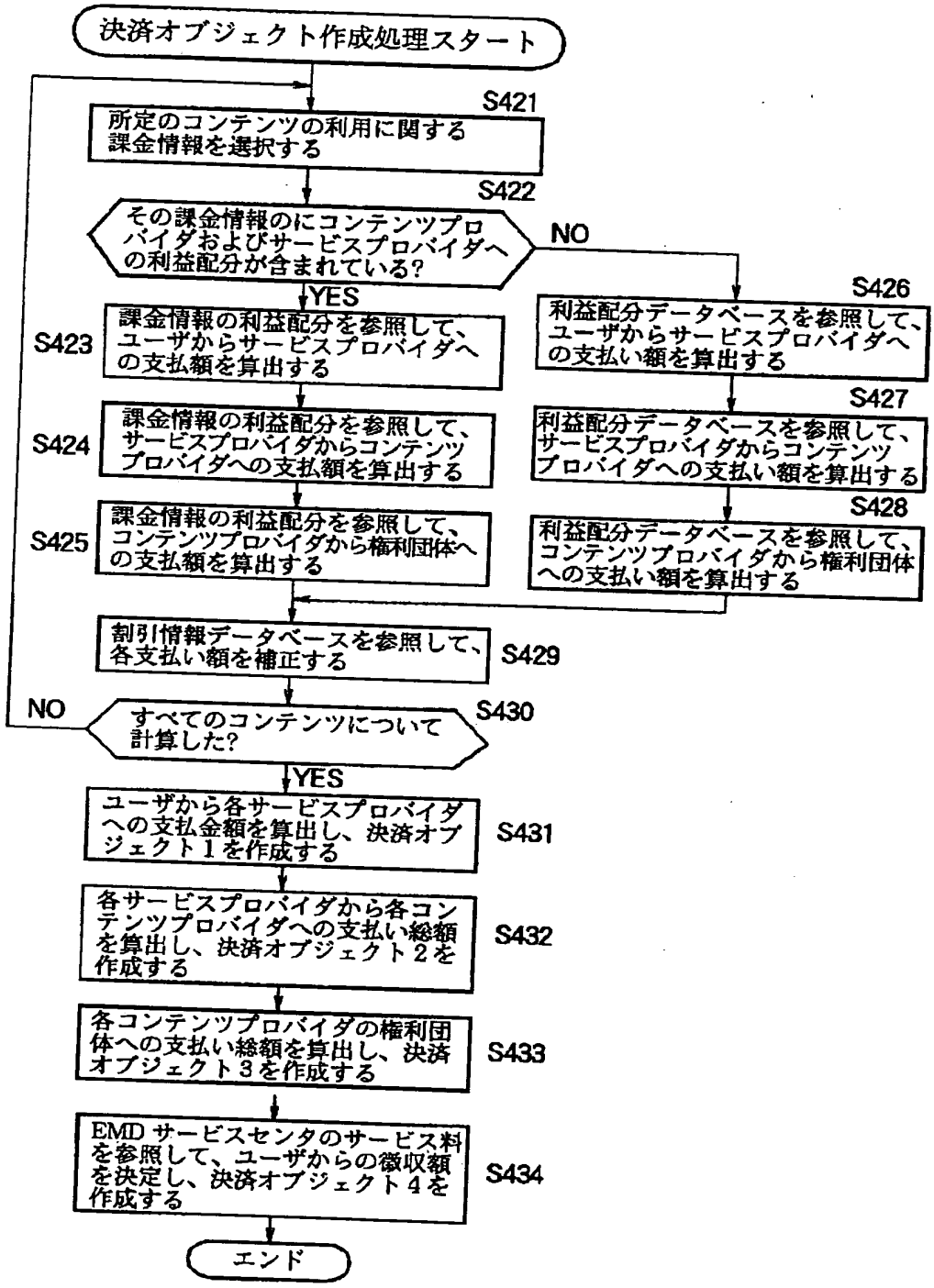
【図５５】


再生処理スタート
S361
HDDから使用許諾条件情報とコンテンツ鍵を読み出す
S362
使用許諾条件情報のハッシュ値を計算する
S363
SAM内のハッシュ値と一致する？
NO
S378
エラー処理
YES
使用許諾条件情報を更新する
S364
使用許諾条件情報のハッシュ値を計算する
S365
ハッシュ値をSAM内に記憶する
S366
使用許諾条件情報をHDDに記憶する
S367
SAMと伸張部で相互認証し、一時鍵が共有される
S368
コンテンツ鍵を保存用鍵で復号する
S369
コンテンツ鍵を一時鍵で暗号化する
S370
コンテンツ鍵を伸張部に送る
S371
コンテンツ鍵を一時鍵で復号する
S372
コンテンツを伸張部に送る
S373
コンテンツ鍵でコンテンツを復号する
S374
コンテンツを伸張する
S375
コンテンツにウォータマークを付加する
S376
コンテンツを出力する
S377
リターン

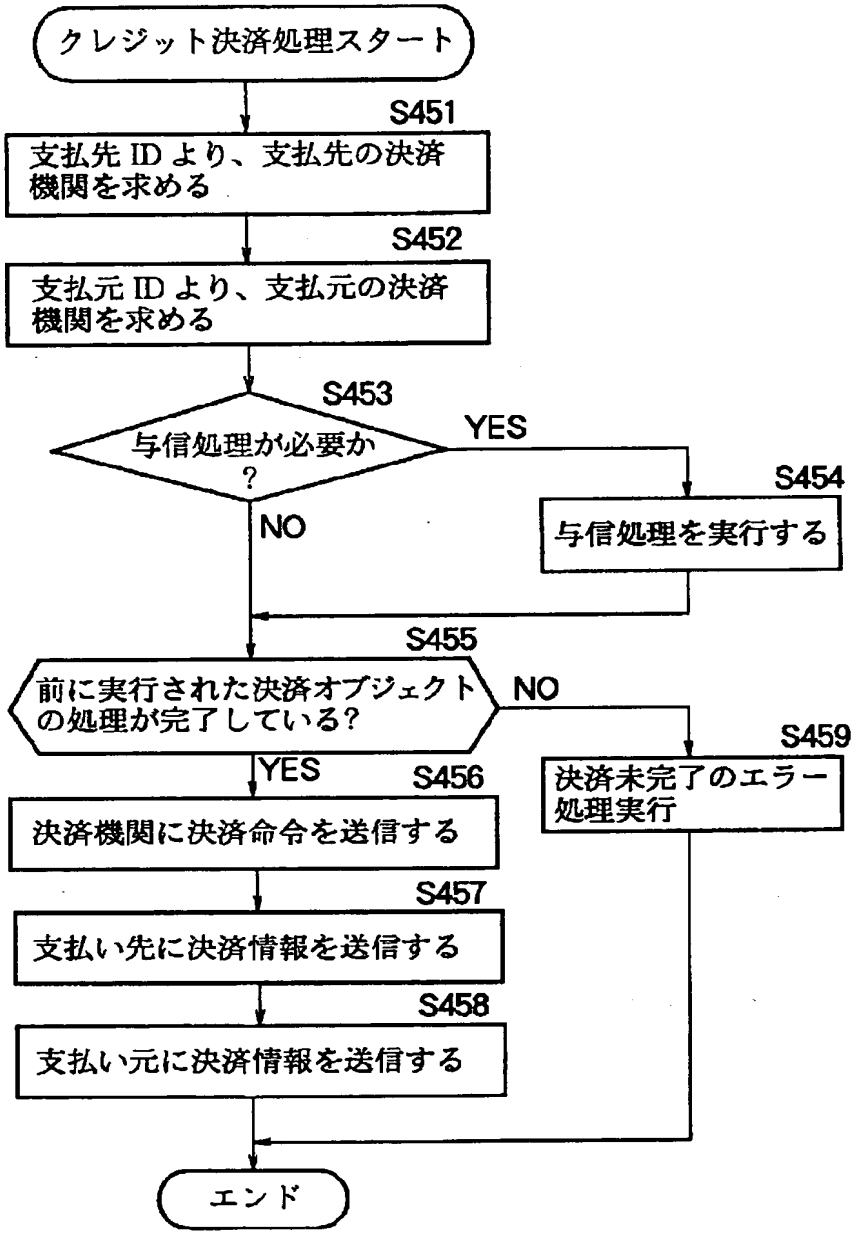
【図５６】


再生処理スタート
S391
HDDから使用許諾条件情報とコンテンツ鍵を読み出す
S392
使用許諾条件情報のハッシュ値を計算する
S393
SAM内のハッシュ値と一致する？
NO
S408
エラー処理
YES
使用許諾条件情報を更新する
S394
使用許諾条件情報のハッシュ値を計算する
S395
ハッシュ値をSAM内に記憶する
S396
使用許諾条件情報をHDDに記憶する
S397
SAMとデコーダで相互認証し、一時鍵が共有される
S398
コンテンツ鍵を保存用鍵で復号する
S399
コンテンツ鍵を一時鍵で暗号化する
S400
コンテンツ鍵をデコーダに送る
S401
コンテンツ鍵を一時鍵で復号する
S402
コンテンツをデコーダに送る
S403
コンテンツ鍵でコンテンツを復号する
S404
コンテンツを伸張する
S405
コンテンツにウォータマークを付加する
S406
コンテンツを出力する
S407
リターン

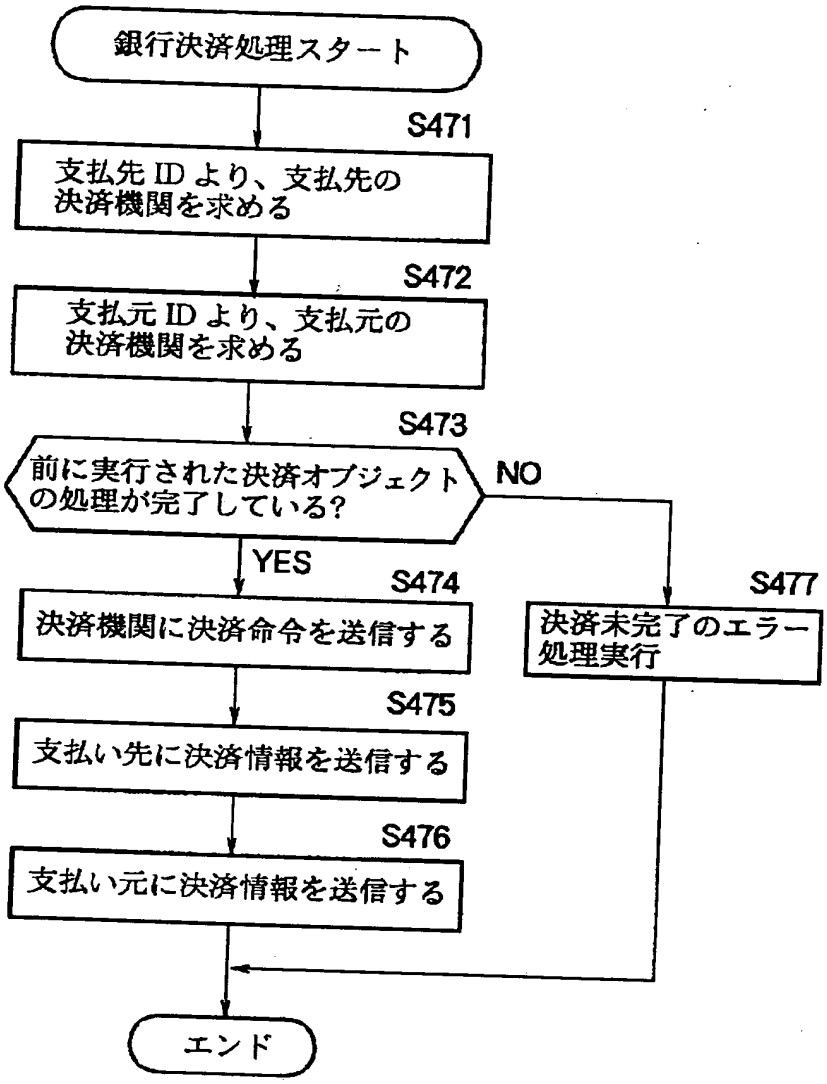
【図５７】


決済オブジェクト作成処理スタート
S421
所定のコンテンツの利用に関する課金情報を選択する
S422
その課金情報のにコンテンツプロバイダおよびサービスプロバイダへの利益配分が含まれている?
NO
YES
S423
課金情報の利益配分を参照して、ユーザからサービスプロバイダへの支払額を算出する
S424
課金情報の利益配分を参照して、サービスプロバイダからコンテンツプロバイダへの支払額を算出する
S425
課金情報の利益配分を参照して、コンテンツプロバイダから権利団体への支払額を算出する
S426
利益配分データベースを参照して、ユーザからサービスプロバイダへの支払い額を算出する
S427
利益配分データベースを参照して、サービスプロバイダからコンテンツプロバイダへの支払い額を算出する
S428
利益配分データベースを参照して、コンテンツプロバイダから権利団体への支払い額を算出する
割引情報データベースを参照して、各支払い額を補正する
S429
NO
すべてのコンテンツについて計算した?
S430
YES
ユーザから各サービスプロバイダへの支払金額を算出し、決済オブジェクト１を作成する
S431
各サービスプロバイダから各コンテンツプロバイダへの支払い総額を算出し、決済オブジェクト２を作成する
S432
各コンテンツプロバイダの権利団体への支払い総額を算出し、決済オブジェクト３を作成する
S433
EMD サービスセンタのサービス料を参照して、ユーザからの徴収額を決定し、決済オブジェクト４を作成する
S434
エンド

【図６１】


クレジット決済処理スタート
S451
支払先 ID より、支払先の決済機関を求める
S452
支払元 ID より、支払元の決済機関を求める
S453
与信処理が必要か？
YES
S454
与信処理を実行する
NO
S455
前に実行された決済オブジェクトの処理が完了している?
NO
S459
決済未完了のエラー処理実行
YES
S456
決済機関に決済命令を送信する
S457
支払い先に決済情報を送信する
S458
支払い元に決済情報を送信する
エンド

【図６２】



フロントページの続き

(51) Int.Cl.'	識別記号	FI		テーマコード' (参考)
Ｈ０４Ｌ　9/32		Ｈ０４Ｍ　15/00	Ｚ	
12/54		Ｈ０４Ｌ　9/00	６７５Ｂ	
12/58		11/20	１０１Ｚ	
// Ｈ０４Ｍ　15/00				

Ｆターム(参考)　5B049 AA05 BB11 BB46 CC31 CC36
CC39 EE02 EE03 FF06 FF09
GG04 GG07 GG10
5B089 GA11 GA21 GB03 HA01 JA40
KA15
5J104 AA07 KA01 KA05 MA02 PA07
PA10
5K025 AA05 BB10 CC01
5K030 HB08 HB21 HC01 KA01

Japanese Patent Application Laid-Open No. 2000-123084

Date of Laid-Open: April 28, 2000

[Title of the Invention]

INFORMATION PROCESSING APPARATUS, INFORMATION PROCESSING METHOD, AND MEDIUM FOR PROVIDING THE SAME

[Abstract]

[Objective] To enable settlement processing and profit-calculation processing to be performed efficiently.

[Means for Solution] A profit-distribution section 16 stores data which specify information, and data which indicate an amount to be paid to each information provider for use of the information. The profit-distribution section 16 calculates the sum total of amounts to be paid to each information provider, on the basis of the stored data. A treasury section 20 instructs a settlement institute to perform settlement for each information provider, on the basis of profit gained by each information provider, which is calculated by the profit-distribution section 16.

[Claims]

[Claim 1] An information processing apparatus which collects, on behalf of information providers, usage fees from users of information provided by said information providers and distributes profits to said information providers, characterized by comprising:

storage means for storing data which specify said information, and data which indicate an amount to be paid to

each of said information providers for use of said information;

calculation means for calculating the sum total of amounts to be paid to each of said information providers, on the basis of data stored in said storage means; and

settlement instruction means for instructing a settlement institute to perform settlement for each of said information providers, on the basis of profits gained by each of said information providers.

[Claim 2] An information processing apparatus as described in claim 1, characterized in that said calculation means further calculates the sum total of amounts to be paid to said information providers.

[Claim 3] An information processing apparatus as described in claim 1, characterized in that said storage means further stores information regarding an amount to be paid to an organization which collects copy-right fees of said information;

said calculation means further calculates the sum total of amounts to be paid to said organization; and

said settlement instruction means further instructs said settlement institute to perform settlement for said organization.

[Claim 4] An information processing apparatus as described in claim 1, characterized in that said storage means further stores data regarding discounts of usage fees of information.

[Claim 5] An information processing apparatus as described

in claim 1, characterized in that said settlement instruction means stores information regarding a settlement institute for each of said information providers.

[Claim 6] An information processing method which collects, on behalf of information providers, usage fees from users of information provided by said information providers and distributes profits to said information providers, characterized by comprising:

a storing step for storing data which specify said information, and data which indicate an amount to be paid to each of said information providers for use of said information;

a calculating step for calculating the sum total of amounts to be paid to each of said information providers, on the basis of data stored in said storing step; and

a settlement instructing step for instructing a settlement institute to perform settlement for each of said information providers, on the basis of profits gained by each of said information providers.

[Claim 7] A provision medium for providing a computer-readable program to an information processing apparatus which collects, on behalf of information providers, usage fees from users of information provided by said information providers and distributes profits to said information providers, said program causing said information processing apparatus to execute processing which comprises:

a storing step for storing data which specify said

information, and data which indicate an amount to be paid to each of said information providers for use of said information;

a calculating step for calculating the sum total of amounts to be paid to each of said information providers, on the basis of data stored in said storing step; and

a settlement instructing step for instructing a settlement institute to perform settlement for each of said information providers, on the basis of profits gained by each of said information providers.

[Detailed Description of the Invention]

[0001]

[Field of the Invention] The present invention relates to an information processing apparatus, an information processing method, and a medium for providing the same. More particularly, the present invention relates to an information processing apparatus, an information processing method, and a medium for providing the same, which collect, on behalf of information providers, usage fees from information users and distribute profits to the information providers.

[0002]

[Prior Art] There exists a system such that encrypted information such as music is transmitted to an information processing apparatus of a user whose has signed a predetermined agreement, and the user decrypts the information on the information processing apparatus and plays back the music or the like. The information provider can

transmit information to a plurality of information providers to thereby provide services.

[0003]

[Problems to be Solved by the Invention] The information provider must enter an agreement with each of a plurality of users and collect usage fees. In addition, settlement processing and profit-calculation processing are wasteful in many aspects.

[0004] In view of the foregoing, an object of the present invention is to perform the settlement processing and profit-calculation processing more efficiently.

[0005]

[Means for Solving the Problems] The information processing apparatus described in claim 1 is characterized by comprising: storage means for storing data which specify the information, and data which indicate an amount to be paid to each of information providers for use of the information; calculation means for calculating the sum total of amounts to be paid to each of the information providers, on the basis of data stored in the storage means; and settlement instruction means for instructing a settlement institute to perform settlement for each of the information providers, on the basis of profits gained by each of the information providers.

[0006] The information processing method described in claim 6 is characterized by comprising: a storing step for storing data which specify the information, and data which indicate an amount to be paid to each of information providers for use

of the information; a calculating step for calculating the sum total of amounts to be paid to each of the information providers, on the basis of data stored in the storing step; and a settlement instructing step for instructing a settlement institute to perform settlement for each of the information providers, on the basis of profits gained by each of the information providers.

[0007] The provision medium described in claim 7 is characterized by providing a computer-readable program which causes an information processing apparatus to execute processing comprising a storing step for storing data which specify the information, and data which indicate an amount to be paid to each of information providers for use of the information; a calculating step for calculating the sum total of amounts to be paid to each of the information providers, on the basis of data stored in the storing step; and a settlement instructing step for instructing a settlement institute to perform settlement for each of the information providers, on the basis of profits gained by each of the information providers.

[0008] In the information processing apparatus described in claim 1, the information processing method described in claim 6, and the provision medium described in claim 7, data which specify information, and data which indicate an amount to be paid to each of information providers for use of the information are stored; the sum total of amounts to be paid to each of the information providers is calculated on the

basis of the stored data; and an instruction is issued to a settlement institute to perform settlement for each of the information providers, on the basis of profits gained by each of the information providers.

[0009]

[Embodiment of the Invention] Hereinbelow, an embodiment of the present invention will be described. In order to show the correspondence between the individual means of the invention described in the Claims and elements in the embodiment described below, in the following description regarding the feature of the present invention, each means is followed by a corresponding element (however, mere example) in the embodiment, enclosed in parentheses. However, this description does not mean that the individual means is limited to the described element.

[0010] An information processing apparatus described in claim 1 comprises storage means (e.g., a profit-distribution section 16 shown in FIG. 2) for storing data which specify information, and data which indicate an amount to be paid to each of information providers for use of the information; calculation means (e.g., the profit-distribution section 16 shown in FIG. 2) for calculating the sum total of amounts to be paid to each of the information providers, on the basis of data stored in the storage means; and settlement instruction means (e.g., a treasury section 20 shown in FIG. 2) for instructing a settlement institute to perform settlement for each of the information providers, on the basis of profit

gained by each of the information providers.

[0011] FIG. 1 is a diagram used for explaining an EMD (Electronic Music Distribution) system to which the present invention is applied. In the system, content distributed to a user refers to digital data whose information is valuable in itself. In the following description, music data are used as an example. An EMD service center 1 transmits a distribution key Kd to a content provider 2, a user home network 5, etc. The EMD service center 1 receives from the user home network 5 charging information produced in accordance with use of content, calculates a usage fee, and distributes profit to the content provider 2 and a service provider 3.

[0012] The content provider 2 holds digitized content. The content provider 2 inserts a watermark (electronic watermark) into the content in order to prove that the content is owned by the content provider 2, compresses and encrypts the content, adds predetermined information to the encrypted content, and transmits it to the service provider 3.

[0013] The service provider 3 adds price information to the content supplied from the content provider 2 and transmits it to the user home network 5 via a network 4, which is formed of a dedicated cable network, the Internet, or a satellite.

[0014] The user home network 5 receives the content and the price information attached thereto from the service provider 3, uses the content through decryption and reproduction, and executes charging processing. Charging information obtained

by the charging process is transmitted to the EMD service center 1 when the user home network 5 obtains a distribution key Kd from the EMD service center 1.

[0015] FIG. 2 is a block diagram showing the functional configuration of the EMD service center 1. A service-provider management section 11 supplies to the service provider 3 information regarding profit distribution. Further, when information (handling policy) which is added to content from the content provider 2 is encrypted information, the service-provider management section 11 transmits a distribution key Kd to the service provider 3. A content-provider management section 12 transmits to the content provider 2 a distribution key Kd and information regarding profit distribution. A copyright management section 13 transmits to an organization which manages copyrights; e.g., JASRAC (Japanese Society for Rights of Authors, Composers and Publishers) information which shows a record of use of the content by the user home network 5. A key server 14 stores distributions keys Kd and supplies the distributions keys Kd to the content provider 2, the user home network 5, etc., via the content-provider management section 12 or a user management section 18. The user management section 18 inputs and stores in a historical-data management section 15 charging information, which is information showing a record of use of content by the user home network 5, price information corresponding to the content, and handling policy corresponding to the content.

[0016] An example in which distribution keys Kd are regularly transmitted from the EMD service center 1 to the content provider 2 and a receiver 51 (which will be described in relation to FIG. 10) which constitutes the user home network 5 will be described with reference to FIGS. 3 to 6. FIG. 3 is a diagram which shows distribution keys Kd held by the EMD service center 1, distribution keys Kd held by the content provider 2, and distribution keys Kd held by the receiver 51, in January, 1998, when the content provider 2 starts provision of content and the receiver 51 constituting the user home network 5 starts use of the content.

[0017] In the example of FIG. 3, each distribution key Kd can be used from the first day to the last day of the corresponding calendar month. For example, a distribution key Kd of version 1 having a value of "aaaaaaaa," which is a random number having a predetermined number of bits, can be used from January 1, 1998 to January 31, 1998 (that is, a content key Kco which is used for encrypting content which the service provider 3 distributes to the user home network 5 during the period from January 1, 1998 to January 31, 1998 is encrypted by use of the distribution key Kd of version 1). A distribution key Kd of version 2 having a value of "bbbbbbbb," which is a random number having a predetermined number of bits, can be used from February 1, 1998 to February 28, 1998 (that is, a content key Kco which is used for encrypting content which the service provider 3 distributes to the user home network 5 during that period is encrypted by

use of the distribution key Kd of version 2). Similarly, a distribution key Kd of version 3 can be used in March, 1998; a distribution key Kd of version 4 can be used in April, 1998; a distribution key Kd of version 5 can be used in May, 1998; and a distribution key Kd of version 6 can be used in June, 1998.

[0018] Before the content provider 2 starts provision of content, the EMD service center 1 transmits to the content provider 2 six distribution keys Kd of version 1 to 6, which can be used in January, 1998 to June, 1998. The content provider 2 receives and stores the six distribution keys Kd. The reason why the content provider 2 stores the distribution keys Kd for six months is that before provision of the content, the content provider 2 requires a certain period for preparation of the content and encryption of a content key.

[0019] Before the receiver 51 starts use of the content, the EMD service center 1 transmits to the receiver 51 three distribution keys Kd of versions 1 to 3 which can be used in January, 1998 to March, 1998. The receiver 51 receives and stores the three distribution keys Kd. The reason why the receiver 51 stores the distribution keys Kd for three months is to avoid a situation such that the user home network 5 cannot utilize the content even within an agreed period during which the content is available, due to problems such that the receiver 51 cannot be connected to the EMD service center 1, and to reduce the frequency of the receiver 51

being connected to the EMD service center 1 and load on the user home network 5.

[0020] During the period from January 1, 1998 to January 31, 1998, the distribution key Kd of version 1 is used among the EMD service center 1, the content provider 2, and the receiver 51, which constitutes the user home network 5.

[0021] Transmission of distribution keys Kd from the EMD service center 1 to the content provider 2 and the receiver 51 on February 1, 1998 will be described with reference to FIG. 4. The EMD service center 1 transmits to the content provider 2 six distribution keys Kd of versions 2 to 7, which can be used from February, 1998 to July, 1998. The content provider 2 receives the six distribution keys Kd and overwrites them on the previously stored distribution keys Kd to thereby store the new distribution keys Kd. The EMD service center 1 transmits to the receiver 51 three distribution keys Kd of versions 2 to 4, which can be used from February, 1998 to April, 1998. The receiver 51 receives the three distribution keys Kd and overwrites them on the previously stored distribution keys Kd to thereby store the new distribution keys Kd. The EMD service center 1 stores the distribution key Kd of version 1 without erasing it. This is to allow use, when an unexpected trouble occurs or a fraudulent activity is performed or discovered, of the distribution key Kd which was used in the past.

[0022] During the period from February 1, 1998 to February 28, 1998, the distribution key Kd of version 2 is used among

the EMD service center 1, the content provider 2, and the receiver 51, which constitutes the user home network 5.

[0023] Transmission of distribution keys Kd from the EMD service center 1 to the content provider 2 and the receiver 51 on March 1, 1998 will be described with reference to FIG. 5. The EMD service center 1 transmits to the content provider 2 six distribution keys Kd of versions 3 to 8, which can be used from March, 1998 to August, 1998. The content provider 2 receives the six distribution keys Kd and overwrites them on the previously stored distribution keys Kd to thereby store the new distribution keys Kd. The EMD service center 1 transmits to the receiver 51 three distribution keys Kd of versions 3 to 5, which can be used from March, 1998 to May, 1998. The receiver 51 receives the three distribution keys Kd and overwrites them on the previously stored distribution keys Kd to thereby store the new distribution keys Kd. The EMD service center 1 stores the distribution key Kd of version 1 and the distribution key Kd of version 2 without erasing them.

[0024] During the period from March 1, 1998 to March 31, 1998, the distribution key Kd of version 3 is used among the EMD service center 1, the content provider 2, and the receiver 51, which constitutes the user home network 5.

[0025] Transmission of distribution keys Kd from the EMD service center 1 to the content provider 2 and the receiver 51 on April 1, 1998 will be described with reference to FIG. 6. The EMD service center 1 transmits to the content

provider 2 six distribution keys Kd of versions 4 to 9, which can be used from April, 1998 to September, 1998. The content provider 2 receives the six distribution keys Kd and overwrites them on the previously stored distribution keys Kd to thereby store the new distribution keys Kd. The EMD service center 1 transmits to the receiver 51 three distribution keys Kd of versions 4 to 6, which can be used from April, 1998 to June, 1998. The receiver 51 receives the three distribution keys Kd and overwrites them on the previously stored distribution keys Kd to thereby store the new distribution keys Kd. The EMD service center 1 stores the distribution key Kd of version 1, the distribution key Kd of version 2, and the distribution key Kd of version 3 without erasing them.

[0026] During the period from April 1, 1998 to April 30, 1998, the distribution key Kd of version 4 is used among the EMD service center 1, the content provider 2, and the receiver 51, which constitutes the user home network 5.

[0027] As described above, since distribution keys Ks for future months are distributed in advance, the user can purchase the content even when the user does not access the center at all during a period of one or two months, and can receive a key by accessing the center at a convenient time.

[0028] The profit-distribution section 16 calculates profits of the EMD service center 1, the content provider 2, and the service provider 3, on the basis of the charging information, price information, and handling policy, which are supplied

from the historical-data management section 15. A mutual authentication section 17 executes mutual authentication, which will be described later, with the content provider 2, the service provider 3, and a predetermined apparatus of the user home network 5.

[0029] The user management section 18 has a user-registration database. When a registration request is issued from the apparatus of the user home network 5, the user management section 18 searches the user-registration database, and, on the basis of the contents of the record, performs processing for registering the apparatus or denying the registration. When the user home network 5 consists of a plurality of apparatuses which can be connected to the EMD service center 1, the user management section 18 designates an apparatus to be used for settlement, on the basis of results of judgment as to whether individual apparatuses can be registered. Further, the user management section 18 transmits to the predetermined apparatus of the user home network 5 a registration list which prescribes conditions of use of the content.

[0030] FIG. 7 shows an example of the user-registration database. A 64-bit ID (Identification Data) peculiar to each apparatus of the user home network 5 is recorded. Further, for each ID (i.e., for each apparatus having the corresponding ID), there is provided information indicating whether the apparatus can perform settlement processing, information indicating whether the apparatus can be

registered, and information indicating whether the apparatus can be connected to the EMD service center 1. The information indicating possibility of registration recorded in the user-registration database is updated at predetermined time intervals, on the basis of information regarding nonpayment of fees, fraudulent processing, etc., provided from the settlement institute (e.g., bank) or the service provider 3. When an apparatus having an ID which is recorded as being not registerable issues a registration request, the user management section 18 denies the registration. Subsequent to this, the apparatus cannot utilize contents of the system.

[0031] The information indicating possibility of settlement processing recorded in the user-registration database indicates whether that apparatus can effect settlement. In the case in which the user home network 5 consists of a plurality of apparatuses which can use content through reproduction or copying thereof, among the plurality of apparatuses, one apparatus which can effect settlement outputs to the EMD service center 1 the charging information, price information, and handling policy for all the apparatuses of the user home network 5 registered in the EMD service center 1. The information indicating possibility of connection with the EMD service center 1 recorded in the user-registration database indicates whether that apparatus can be connected to the EMD service center 1. An apparatus which is recorded as being unconnectable outputs charging

information, etc. to the EMD service center 1 via other apparatuses of the user home network 5.

[0032] The user management section 18 receives charging information, price information, and handling policy supplied from apparatuses of the user home network 5 and outputs them to the historical-data management section 15. Further, through predetermined processing (at predetermined timing), the user management section 18 supplies distribution keys Kd to the user home network 5.

[0033] A charge billing section 19 calculates a charge for the user, on the basis of charging information, price information, and handling policy supplied from the historical-data management section 15, and supplies calculation results to the treasury section 20. The treasury section 20 communicates with an unillustrated external bank or a like organization in order to perform settlement processing, on the basis of amounts of money to be paid to and usage fees to be collected from the user, the content provider 2, and the service provider 3. An auditor section 21 audits accuracy of the charging information, price information, and handling policy supplied from the apparatus of the user home network 5 (i.e., whether fraudulence is present therein).

[0034] FIG. 8 is a block diagram showing the functional configuration of the content provider 2. A content server 31 stores content to be supplied to users and supplies it to a watermark adding section 32. The watermark adding section 32

adds a watermark to the content supplied from the content server 31 and sends it to a compression section 33. The compression section 33 compresses the content supplied from the watermark adding section 32 in accordance with an ATRAC2 (Adaptive Transform Acoustic Coding 2) (Trademark) scheme or any other scheme and supplies the compressed content to an encryption section 34. The encryption section 34 encrypts the content compressed by the compression section 33 in accordance with a common key cryptosystem such as DES (Data Encryption Standard) and by use, as a key, of a random number supplied from a random-number generation section 35 (hereinafter, this random number will be referred to as a content key Kco), and outputs the result of the encryption to a secure container creation section 38.

[0035] The random-number generation section 35 outputs to the encryption section 34 and the encryption section 36 a random number having a predetermined number of bits and serving as a content key Kco. The encryption section 36 encrypts the content key Kco in accordance with a common key cryptosystem such as DES and by use of a distribution key Kd supplied from the EMD service center 1, and outputs the results of encryption to the secure container creation section 38.

[0036] DES is an encryption system which processes plain text while handling 64 bits as a single block. The processing of DES consists of a portion (data scrambling section) for scrambling plain text and converting it into

encrypted text, and a portion (key processing section) for generating from a common key a key (extended key) to be used in the data scrambling section. Since the entire algorithm of DES is opened to the public, here, the basic processing of the data scrambling section will be described briefly.

[0037] First, 64 bits of plain text are divided into upper 32 bits H_0 and lower 32 bits L_0. A 48-bit extended key K_1 supplied from the key processing section and the lower 32 bits L_0 are used as inputs in order to calculate an output of an F-function in which the lower 32 bits L_0 have been scrambled. The F-function consists of "replacement" for replacing numerals in accordance with a predetermined rule and "transposition" for transposing bit positions in accordance with a predetermined rule. Subsequently, the upper 32 bits H_0 and the F-function output are subjected to exclusive-OR, and the result is used as L_1. L_0 is used as H_1.

[0038] On the basis of the upper 32 bits H_0 and the lower 32 bits L_0, the above-described processing is repeated 16 times; and the thus-obtained upper 32 bits H_{16} and lower 32 bits L_{16} are output as encrypted text. Decryption is performed to inversely follow the above-described steps, while using the common key used in the encryption.

[0039] A policy storage section 37 stores a policy on handling of content, and outputs to the secure container creation section 38 a handling policy corresponding to content to be encrypted. The secure container creation section 38 creates a content-provider secure container and

supplies it to the service provider 3. The content-provider secure container includes encrypted content; an encrypted content key Kco; a handling policy; a signature created from hash values of the encrypted content, the encrypted content key Kco, and the handling policy; and a certificate including a public key Kpcp of the content provider 2. Before receiving a distribution key Kd from the EMD service center 1, a mutual authentication section 39 mutually authenticates with the EMD service center 1. Further, before transmission of the content-provider secure container to the service provider 3, the mutual authentication section 39 mutually authenticates with the service provider 3.

[0040] Signature refers to data which are attached to data or a certificate, which will be described later, in order to enable check for tampering and perform author authentication. A hash value is obtained by use of a hash function and on the basis of data to be transmitted; and the thus-obtained hash value is encrypted by a private key of a public key cryptosystem.

[0041] The hash function and signature collation will be described. The hash function is a function which receives predetermined data to be transmitted, compresses the data into data having a predetermined bit length, and outputs the result as a hash value. The hash function has features such that an input is difficult to predict from a hash value (output), that when a certain bit of data input to the hash function changes, many bits of the hash value change, and

that finding input data having the same hash value is difficult.

[0042] A receiving person who has received a signature and data decrypts the signature by use of a public key of the public key cryptosystem to obtain a resultant value (hash value). Further, a hash value of the received data is calculated; and a judgment is made as to whether the calculated hash value is equal to the hash value obtained through decryption of the signature. When the hash value of the transmitted data is judged to be equal to the decrypted hash value, this means that the received data have not been subjected to tampering and have been transmitted from a transmitting person who holds a private key corresponding to the public key. Examples of the hash function for signature include MD4, MD5, and SHA-1.

[0043] Next, the public key cryptosystem will be described. In contrast to a common key cryptosystem in which the same key (common key) is used for encryption and decryption, in the public key cryptosystem, a key used for encryption differs from a key used for decryption. When the public key cryptosystem is employed, even when one of the keys is disclosed, the other can be kept secret. A key which may be opened to the public is called a public key; and a key which is kept secret is called a private key.

[0044] RSA (Rivest-Shamir-Adleman) cryptosystem, which is a typical example of the public key cryptosystem, will be described briefly. First, two sufficiently large prime

numbers p and q are obtained, and then a product n of p and q is obtained. The least common multiple L of (p-1) and (q-1) is calculated. Subsequently, a number e which is at least 3 but less than L and which shares no common factors with L (i.e., 1 is the only natural number by which both e and L can be divided evenly) is obtained.

[0045] Subsequently, a multiplicative inverse element d of e modulo L is obtained. That is, ed=1 mod L holds among d, e, and L, and d can be calculated through the Euclidean algorithm. n and e are used as public keys; and p, q, and d are used as private keys.

[0046] An encrypted text C is calculated from a plain text M through processing of formula (1).

$$C = M^e \bmod n \qquad (1)$$

[0048] The encrypted text C is decrypted to the plain text M through processing of formula (2).

$$M = C^d \bmod n \qquad (2)$$

[0048] Although proof is omitted, the reason why a plain text can be converted to an encrypted text by the RSA cryptosystem and the encrypted text can be decrypted is based on Fermat's theorem, and formula (3) stands.

$$M = C^d = (M^e)^d = M^{(ed)} \bmod n \qquad (3)$$

[0049] If the private keys p and q are known, the private key d can be calculated from the public key e. However, if the number of digits of the public key n is increased to a degree such that factorization of n in prime numbers is difficult from the viewpoint of calculation volume, even if the public

key n is known, the private key d cannot be calculated from the public key e, making decryption impossible. As described above, in the RSA cryptosystem, the key used for decryption is made different from the key used for encryption.

[0050] Further, the elliptic-curve cryptosystem, which is another example of the public key cryptosystem, will be described briefly. Assume that a certain point on an elliptic curve $y^2 = X^3 + ax+b$ is denoted by B. Addition of points on the elliptic curve is defined, and nB represents a result of n times of addition of B. Similarly, subtraction is defined. It has been proved that calculating n from B and nB is difficult. B and nB are used as public keys; and n is used as a private key. Encrypted texts C1 and C2 are calculated from a plain text M by use of a random number r and the public key, through processing represented by formulas (4) and (5).

$$C1 = M+rnB \qquad (4)$$

$$C2 = rB \qquad (5)$$

[0051] The encrypted texts C1 and C2 are decrypted to the plain text M through processing of formula (6).

$$M = C1 - nC2 \qquad (6)$$

[0052] Only a person who has the private key n can decrypt the encrypted texts. As described above, as in the case of the RSA cryptosystem, when the elliptic-curve cryptosystem is employed, the key used for decryption can be made different from the key used for encryption.

[0053] FIG. 9 is a block diagram showing the functional

structure of the service provider 3. A content server 41 stores encrypted content supplied from the content provider 2 and supplies it to a secure container creation section 44. A pricing section 42 creates price information on the basis of a handling policy corresponding to the content and supplies it to the secure container creation section 44. A policy storage section 43 stores the handling policy of the content supplied from the content provider 2 and supplies it to the secure container creation section 44. Before receiving a content-provider secure container from the content provider 2, a mutual authentication section 45 mutually authenticates with the content provider 2. Further, before transmission of a service-provider secure container to the user home network 5, the mutual authentication section 45 mutually authenticates with the user home network 5. When the content provider 2 supplies the handling policy after encryption with a distribution key Kd, the mutual authentication section 45 mutually authenticates with the EMD service center 1, before reception of the distribution key Kd from the EMD service center 1.

[0054] FIG. 10 is a block diagram showing the configuration of the user home network 5. The receiver 51 receives a service-provider secure container including content from the service provider 3 via the network 4; and decrypts, extends, and reproduces the content.

[0055] A communication section 61 communicates with the service provider 3 and the EMD service center 1 via the

network 4 to thereby receive information therefrom and transmit information thereto. A SAM (Secure Application Module) 62 mutually authenticates with the service provider 3 or the EMD service center 1; decrypts a cipher of the content or encrypts the content; and stores the distribution key Kd and other data. An extension section 63 decrypts the cipher of the content, extends it in accordance with the ATRAC2 scheme, and inserts a predetermined watermark into the content. An IC (Integrated Circuit)-card interface 64 converts the signal from the SAM 62 into a predetermined form and outputs the result to an IC card 55 attached to the receiver 51; and converts the signal from the IC card 55 into a predetermined form and outputs the result to the SAM 62.

[0056] The SAM 62——which mutually authenticates with the service provider 3 or the EMD service center 1, performs charging processing, decrypts and encrypts the content key Kco, and stores predetermined data such as information regarding conditions for permission of use (hereinafter referred to as "conditions-for-use information")——includes a mutual authentication module 71, a charging processing module 72, a storage module 73, and a decryption/encryption module 74. The SAM 62 is formed of a single chip IC dedicated for cipher processing which has a multilayer structure such that an internal memory cell is sandwiched between dummy layers of, for example, aluminum and has characteristics (tampering resistance) which make it difficult to illegally read data from the outside; such as a

narrow operable voltage range and a narrow operable frequency range.

[0057] The mutual authentication module 71 mutually authenticates with the service provider 3 or the EMD service center 1; and, if necessary, supplies a temporary key Ktemp (session key) to the decryption/encryption module 74. The charging processing module 72 generates charging information and conditions-for-use information, from the handling policy and price information (and handling control information in some cases) contained in the service-provider secure container received from the service provider 3; and outputs them to the storage module 73 or a HDD (Hard Disk Drive) 52. The storage module 73 stores various data such as the charging information and a distribution key Kd supplied from the charging processing module 72 or the decryption/encryption module 74. When any other function block performs predetermined processing, the storage module 73 supplies the distribution key Kd and other data to that block.

[0058] The decryption/encryption module 74 includes a decryption unit 91, a random-number generation unit 92, and an encryption unit 93. The decryption unit 91 decrypts an encrypted content key Kco with a distribution key Kd and outputs it to the encryption unit 93. The random-number generation unit 92 generates a random number having a predetermined number of digits and outputs the random number to the encryption unit 93 and the storage module 73 as a save

key Ksave. When the save key Ksave is already generated and stored, generation of the key is not required. The encryption unit 93 encrypts the decrypted content key Kco with the save key Ksave and outputs it to the HDD 52. When the content key Kco is transmitted to the extension section 62, the encryption unit 93 encrypts the content key Kco with the temporary key Ktemp.

[0059] The extension section 63——which decrypts and extends the content and adds a predetermined watermark to the content——includes a mutual authentication module 75, a decryption module 76, a decryption module 77, an extension module 78, and a watermark addition module 79. The mutual authentication module 75 mutually authenticates with the SAM 62 and outputs the temporary key Ktemp to the decryption module 76. The decryption module 76 decrypts the content key Kco——which was encrypted with the temporary key Ktemp——with the temporary key Ktemp and outputs it to the decryption module 77. The decryption module 77 decrypts the content stored in the HDD 52 with the content key Kco and outputs it the extension module 78. The extension module 78 extends the decrypted content in accordance with ATRAC2 or any other scheme and outputs it to the watermark addition module 79. the watermark addition module 79 inserts into the content a predetermined watermark specifying the receiver 51 and outputs it to a recorder 53; and outputs the content to an unillustrated speaker to thereby reproduce music.

[0060] The HDD 52 records thereon the content supplied from

the service provider 3. The recorder 53——which records the content supplied from the service provider 3 on an attached optical disk (not shown) and reproduces the content——includes a record/reproduction section 65, an SAM 66, and an extension section 67. The record/reproduction section 65 includes an optical disk attached thereto and adapted to record the content on the optical disk and reproduce the content from the optical disk. The SAM 66 has the same function as that of the SAM 62, and therefore repeated description is omitted. The extension section 67 has the same function as that of the extension section 63, and therefore repeated description is omitted. An MD (Mini Disk; trademark) drive 54 records the content supplied from the service provider 3 on an attached MD (not shown) and reproduces the content from the MD.

[0061] The IC card 55 is attached to the receiver 51 and stores predetermined data such as an equipment ID and the distribution key Kd stored in the storage module 73. In an example case in which a user has purchased a new receiver 51 and uses it in place of the previous receiver 51, the user first stores in the IC card 55 predetermined data such as the distribution key Kd which are stored in the storage module 73 of the previous receiver 51. Next, the user attaches the IC card 55 to the new receiver 51 and operates the receiver 51 in order to register the new receiver 51 in the user management section 18 of the EMD service center 1. On the basis of the data (ID of the previous receiver 51, etc.)

stored in the IC card 55, the user management section 18 of the EMD service center 1 searches the database held in the user management section 18 to obtain data in relation to the user, such as the name of the user, and the number of a credit card used for payment of usage fees. On the basis of the data, the user management section 18 executes registration processing. Therefore, the user is not required to input data, which is cumbersome. The IC card 55 includes a mutual authentication module 80 and a storage module 81. The mutual authentication module 80 mutually authenticates with the SAM 62. The storage module 81 stores the data supplied from the SAM 62 via the IC-card interface 64 and outputs the stored data to the SAM 62.

[0062] FIG. 11 is a block diagram showing another configuration of the user home network 5. The receiver 51 and the recorder 53 in the present configuration do not have the extension sections 63 and 67 shown in FIG. 10. Instead, a decoder 56 connected to the recorder 53 provides the same function as that provided by the extension section 63 or 67. The remaining sections and modules have the same configurations as those in FIG. 10.

[0063] The decoder 56——which decrypts and extends the content and adds a watermark to the content——includes a mutual authentication module 101, a decryption module 102, a decryption module 103, an extension module 104, and a watermark addition module 105. The mutual authentication module 101 mutually authenticates with the SAM 62 or the SAM

66 and outputs the temporary key Ktemp to the decryption module 102. The decryption module 102 decrypts the content key Kco——which was encrypted with the temporary key Ktemp and is output from the SAM 62——with the temporary key Ktemp and outputs it to the decryption module 103. The decryption module 103 decrypts the content stored in the HDD 52 with the content key Kco and outputs it the extension module 104. The extension module 104 extends the decrypted content in accordance with ATRAC2 or any other scheme and outputs it to the watermark addition module 105. the watermark addition module 105 inserts into the content a predetermined watermark specifying the decoder 56 and outputs it to the recorder 53; and outputs the content to an unillustrated speaker to thereby reproduce music.

[0064] FIG. 12 is a diagram used for describing information which is exchanged among the EMD service center 1, the content provider 2, the service provider 3, and the user home network 5. The content provider 2 stores encrypted content, an encrypted content key Kco, a handling policy, and a signature in a content-provider secure container (details of which will be described with reference to FIG. 13); attaches a certificate of the content provider 2 (details of which will be described with reference to FIG. 14) to the content-provider secure container; and transmits the content-provider secure container to the service provider 3. Further, the content provider 2 transmits to the EMD service center 1 the handling policy and the signature to which the certificate of

the content provider 2 is attached.

[0065] The service provider 3 generates price information on the basis of the handling policy contained in the received content-provider secure container, and stores the encrypted content, the encrypted content key Kco, the handling policy, the price information, and the signature in a service-provider secure container (details of which will be described with reference to FIG. 15); attaches a certificate of the service provider 3 (details of which will be described with reference to FIG. 16) to the service-provider secure container; and transmits the service-provider secure container to the user home network 5. Further, the service provider 3 transmits to the EMD service center 1 the price information and the signature to which the certificate of the service provider 3 is attached.

[0066] The user home network 5 generates use-permission information from the handling policy contained in the received service-provider secure container, and uses the content in accordance with the use-permission information. When the content key Kco is decrypted in the user home network 5, charging information is generated. At a predetermined timing, the charging information is encrypted, and the handling policy and the signature are attached to the encrypted charging information, which is then transmitted to the EMD service center 1.

[0067] The EMD service center 1 calculates a usage fee on the basis of the charging information and the handling policy

and further calculates respective profits of the EMD service center 1, the content-provider secure container 2, and the service provider 3. Moreover, the EMD service center 1 compares the handling policy received from the content provider 2, the price information received from the service provider 3, and the charging information and the handling policy received from the user home network 5 in order to check (audit) whether illegal conduct such as tampering with the handling policy or illegal price increase has occurred in the service provider 3 or the user home network 5.

[0068] FIG. 13 is a diagram used for describing the content-provider secure container. The content-provider secure container includes content encrypted by use of a content key Kco; the content key Kco encrypted by use of a distribution key Kd; a handling policy; and a signature. The signature is data which are obtained as follows. A hash function is applied to the content encrypted by use of the content key Kco, the content key Kco encrypted by use of the distribution key Kd, and the handling policy in order to obtain a hash value, which is then encrypted by use of a private key Kscp of the content provider 2.

[0069] FIG. 14 is a diagram used for describing the certificate of the content provider 2. The certificate of the content provider 2 includes a version number of the certificate; a serial number of the certificate which an authentication office has allocated to the content provider 2; an algorithm and parameters used in the signature; the

name of the authentication office; a valid term of the certificate; the name of the content provider 2; the public key Kpcp of the content provider; and a signature. The signature is data which are obtained as follows. A hash function is applied to the version number of the certificate; the serial number of the certificate which the authentication office has allocated to the content provider 2; the algorithm and parameters used in the signature; the name of the authentication office; the valid term of the certificate; the name of the content provider 2; and the public key Kpcp of the content provider in order to obtain a hash value, which is then encrypted by use of a private key Ksca of the authentication office.

[0070] FIG. 15 is a diagram used for describing the service-provider secure container. The service-provider secure container includes the content encrypted by use of the content key Kco; the content key Kco encrypted by use of the distribution key Kd; the handling policy; price information; and a signature. The signature is data which are obtained as follows. A hash function is applied to the content encrypted by use of the content key Kco, the content key Kco encrypted by use of the distribution key Kd, the handling policy, and the price information in order to obtain a hash value, which is then encrypted by use of a private key Kssp of the service provider 3.

[0071] FIG. 16 is a diagram used for describing the certificate of the service provider 3. The certificate of

the service provider 3 includes a version number of the certificate; a serial number of the certificate which an authentication office has allocated to the service provider 3; an algorithm and parameters used in the signature; the name of the authentication office; a valid term of the certificate; the name of the service provider 3; the public key Kpsp of the service provider; and a signature. The signature is data which are obtained as follows. A hash function is applied to the version number of the certificate; the serial number of the certificate which the authentication office has allocated to the service provider 3; the algorithm and parameters used in the signature; the name of the authentication office; the valid term of the certificate; the name of the service provider 3; and the public key Kpsp of the service provider in order to obtain a hash value, which is then encrypted by use of the private key Ksca of the authentication office.

[0072] FIG. 17 is a diagram showing a handling policy, price information, and conditions-for-use information. The content provider 2 has a handling policy for each piece of content, and the handling policy shows items which the user home network 5 can utilize. For example, the handling policy of FIG. 17(A) permits the user home network 5 to perform reproduction and multicopying of content but does not permit the user home network 5 to perform single copying of the content.

[0073] FIG. 18 is a diagram used for describing multicopying

and single copying. A user can perform single copying or multicoping when the user has purchased permission for using content whose copying is permitted under conditions-for-use information. Multicopying refers to making a plurality of copies. However, as shown in FIG. 18(A), the user cannot (is not permitted to) make a copy of a copy. Single copying refers to making a single copy. In the case of single copying as well, as shown in FIG. 18(B), the user cannot (is not permitted to) make a copy of a copy.

[0074] As shown in FIG. 17(B), the service provider 3 adds price information to the handling policy supplied from the content provider 2. For example, the price information shown in FIG. 17(B) indicates that usage fee for reproduction of the content is 150 yen and that usage fee for multicopying is 80 yen. Although not exemplified in FIG. 17, price information for single copying indicates usage fee for making a single copy, and in an example case in which the user performs copying three times, the user pays a fee three times that for single copying. Multicopying or single copying is permitted for only content for which copying is permitted under conditions-for-use information and for which the user has purchased permission for use.

[0075] When the user selects some of the usable items of the content (FIG. 17(B)) indicated by the handling policy supplied from the service provider 3, the user home network 5 stores conditions-for-use information (FIG. 17(C)) which indicates the item(s) selected by the user. For example, the

conditions-for-use information of FIG. 17(C) permits the user home network 5 to reproduce the content but does not permit the user home network 5 to perform single copying and multicopying.

[0076] FIG. 19 is a diagram used for describing a handling policy and price information. This example differs from the example shown in FIG. 17 in that the content provider 2 adds information regarding profit distribution to the handling policy, and the service provider 3 adds the information regarding profit distribution to the price information. In contrast to the example of FIG. 17, in the example of FIG. 19, information indicating that the content provider 2 can obtain a profit of 70 yen from a user's use in the form of reproduction of the content and a profit of 40 yen from a user's use in the form of multicopying is added (FIG. 19(A)). Further, profit-distribution information indicating that the service provider 3 can obtain a profit of 60 yen from a user's use in the form of reproduction of the content and a profit of 30 yen from a user's use in the form of multicopying is added (FIG. 19(B)). An amount of money (e.g., 20 yen) obtained through subtraction of a profit (e.g., 70 yen) of the content provider 2 and a profit (e.g., 60 yen) of the service provider 3 from a price (e.g., 150 yen) is a profit of the EMD service center 1. The EMD service center 1 obtains charging information (FIG. 19(C) which shows the use of the content by the user home network 5. The EMD service center 1 further obtains a handling policy, profit-

distribution ratios, and price information via the user home network 5, to thereby calculate the respective profits of the content provider 2, the service provider 3, and the EMD service center 1).

[0077] FIG. 20 is a diagram used for describing a handling policy, price information, and conditions-for-use information for the case in which a plurality of manners of reproduction of the content are set. In the example of FIG. 20(A), the service provider 3 sets the handling policy and price information to reflect a plurality of manners of reproduction of the content; i.e., limitless reproduction, reproduction within a limited number of times (5 times in this example), and reproduction within a limited period (until December 31, 1998 in this case). When a user uses the content while selecting the reproduction which is limited to 5 times, "5" is recorded, as a maximum number of times, in the conditions-for-use information of the user home network 5 as shown in FIG. 20(B) in a state in which the user has not yet reproduced the content after receipt thereof. This value indicating the maximum number of times is decremented every time the content is reproduced (used) in the user home network 5. For example, after the content is reproduced three times, the value is changed to "2" as shown in FIG. 20(C). When the value of the number limit becomes "0," the user home network 5 becomes unable to further reproduce and use the content.

[0078] FIG. 21 is a diagram showing another example of

information exchanged among the EMD service center 1, the content provider 2, the service provider 3, and the user home network 5. The example of FIG. 21 differs from the example of FIG. 12 in that the service provider 3 creates handling control information on the basis of the handling policy received from the content provider 2. The handling control information is stored in the service-provider secure container together with the content and other data and is then transmitted to the user home network 5 and the EMD service center 1. Further, the handling control information is transmitted from the user home network 5 to the EMD service center 1 together with charging information and the handling policy.

[0079] FIG. 22 is a diagram used for describing a service-provider secure container used in the example of FIG. 21. The service-provider secure container includes a content encrypted by use of a content key Kco; the content key Kco encrypted by use of a distribution key Kd; a handling policy; handling control information; price information; and a signature. The signature is data which are obtained as follows. A hash function is applied to the content encrypted by use of the content key Kco, the content key Kco encrypted by use of the distribution key Kd, the handling policy, the handling control information, and the price information in order to obtain a hash value, which is then encrypted by use of a private key Kssp of the service provider 3.

[0080] FIG. 23 shows the details of the handling policy,

handling control information, and conditions-for-use information in the example of FIG. 21. In the example of FIG. 23, the handling policy of the content provider 2 (FIG. 23(A)) does not have a form such that simple addition of price information enables referral to price information through comparison between the handling policy and the price information. In view of the foregoing, on the basis of the handling policy, there is produced handling control information having a form which enables referral to price information through comparison between the handling policy and the price information; and the price information is added to the handling control information, which is then transmitted to the user home network 5 (FIG. 23(B)). The user home network 5 produces conditions-for-use information from the received information (FIG. 23 (C)). As compared to the case of FIG. 12, the content provider 2 in FIG. 23 has an advantage in that the handling policy that the content provider 2 is required to record is of a further reduced amount of data.

[0081] FIG. 24 is a diagram showing another example of content and information accompanying the content, which are exchanged among the EMD service center 1, the content provider 2, the service provider 3, and the user home network 5. The example of FIG. 24 differs from the example of FIG. 21 in that in the example of FIG. 24 a handling policy, handling control information, price information, and charging information are encrypted by means of a public cryptosystem

and are then transmitted. As compared to the case of FIG. 21, the system in FIG. 24 has enhanced safety against attack from outside the system.

[0082] FIG. 25 is a diagram used for describing a content-provider secure container used in the example of FIG. 24. The content-provider secure container includes content encrypted by use of a content key Kco; the content key Kco encrypted by use of a distribution key Kd; a handling policy encrypted by use of the distribution key Kd; and a signature. The signature is data which are obtained as follows. A hash function is applied to the content encrypted by use of the content key Kco, the content key Kco encrypted by use of the distribution key Kd, and the handling policy encrypted by use of the distribution key Kd in order to obtain a hash value, which is then encrypted by use of a private key Kscp of the content provider 2.

[0083] FIG. 26 is a diagram used for describing a service-provider secure container used in the example of FIG. 24. The service-provider secure container includes the content encrypted by use of the content key Kco; the content key Kco encrypted by use of the distribution key Kd; the handling policy encrypted by use of the distribution key Kd; handling control information encrypted by use of the distribution key Kd; price information encrypted by use of the distribution key Kd; and a signature. The signature is data which are obtained as follows. A hash function is applied to the content encrypted by use of the content key Kco, the content

key Kco encrypted by use of the distribution key Kd, the handling policy encrypted by use of the distribution key Kd, the handling control information encrypted by use of the distribution key Kd, and the price information encrypted by use of the distribution key Kd in order to obtain a hash value, which is then encrypted by use of a private key Kssp of the service provider 3.

[0084] FIG. 27 is a diagram used for describing another operation of the EMD service center 1 for collecting data necessary for settlement processing, from the content provider 2, the service provider 3, and the user home network 5. The content provider 2 transmits to the EMD service center 1 content-provider registration data consisting of the name of the content provider 2, a content ID, a profit of a proprietor organization corresponding to the content ID, and the number of a bank account of the content provider 2; and the content-provider management section 12 of the EMD service center 1 receives the content-provider registration data. Upon reception of the content-provider registration data, the content-provider management section 12 of the EMD service center 1 generates a content-provider ID and registers the content-provider registration data, together with the content-provider ID, into a profit-distribution database. Further, the content-provider management section 12 transmits the content-provider ID to the content provider 2. The content provider 2 receives and stores the content-provider ID.

[0085] The service provider 3 transmits to the EMD service center 1 service-provider registration data consisting of the name of the service provider 3, a content ID, and the number of a bank account of the service provider 3; and the service-provider management section 11 of the EMD service center 1 receives the service-provider registration data. Upon reception of the service-provider registration data, the service-provider management section 11 of the EMD service center 1 generates a service-provider ID and transmits the service-provider ID to the service provider 3. The service provider 3 receives and stores the content-provider ID.

[0086] The user home network 5 transmits to the EMD service center 1 user registration data consisting of the name of a user and the number of a bank account of the user; and the user management section 18 of the EMD service center 1 receives the user registration data. Upon reception of the user registration data, the user management section 18 of the EMD service center 1 generates a user ID, stores the user registration data together with the user ID, and transmits the user ID to the user home network 5. The user home network 5 receives and stores the user ID.

[0087] FIG. 28 is a diagram showing an example of the profit-distribution database. Distribution of profit to the proprietor organization corresponding to each content ID is stored in the profit-distribution database. The distribution of profit to the proprietor organization corresponding to a content ID indicates a ratio of distribution to the

proprietor organization of a profit which is produced when content corresponding to the content ID is utilized by the user.

[0088] In the example profit-distribution database shown in FIG. 28, when content whose content ID is 1 is provided from the service provider 3 to the user, 10% of the profit produced from utilization of the content by the user is distributed to the proprietor organization. Similarly, when content whose content ID is 2 is used by the user, 20% of the profit produced from utilization of the content by the user is distributed to the proprietor organization.

[0089] FIG. 29 shows a content-fee discount table stored in the profit-distribution section 16 of the EMD service center 1. The content-fee discount table stores discount rates of usage fees to be paid by users for each combination of a content ID and a content-provider ID. The discount table is designed to store other information items such as periods during which individual discount rates are applied.

[0090] A usage fee for content whose content ID is 1 and which is supplied from a content provider 2 whose content-provider ID is 1 is discounted at a rate of 0.02 during a period from September, 1998 to December, 1998. A usage fee for content whose content ID is 2 and which is supplied from a content provider 2 whose content-provider ID is 1 is discounted at a rate of 0.03. A usage fee for content which has a content ID other than 1 and 2 and which is supplied from a content provider 2 whose content-provider ID is 1 is

discounted at a rate of 0.01. A usage fee for content whose content ID is 3 and which is supplied from a content provider 2 whose content-provider ID is 2 is discounted at a rate of 0.05. A usage fee for content whose content ID is 1 and which is supplied from a service provider 3 whose service-provider ID is 1 is discounted at a rate of 0.03. A usage fee for content whose content ID is 4 and which is supplied from a service provider 3 whose service-provider ID is 2 is discounted at a rate of 0.01.

[0091] FIG. 30 shows a user's usage-fee table stored in the charge billing section 19 of the EMD service center 1. The user's usage-fee table stores a usage fee which the user pays to the EMD service center 1. A monthly basic charge in the user's usage-fee table indicates a fixed usage fee which the user pays to the EMD service center 1 each month. An adjustment amount indicates a discount rate that is applied to the monthly basic charge during a predetermined special period and a discount rate that is applied to the monthly basic charge when the usage fee, including usage fees of contents, exceeds a predetermined amount.

[0092] In the example user's usage-fee table shown in FIG. 30, the monthly basic charge is 1000 yen; and the monthly basic charge is discounted by 10% during a period from August, 1998 to September, 1998. Further, when the usage fee, including usage fees for contents, exceeds 3000 yen, the monthly basic charge is discounted by 5%.

[0093] A usage fee for content is calculated from the

profit-distribution database or charging information; a discount amount is subtracted from the thus-calculated content usage fee; and the fee for use of the EMD service center 1 is added thereto, whereby a usage fee to be paid by a corresponding user is calculated.

[0094] FIG. 31 shows an operation of the EMD service center 1 when the EMD service center 1 receives charging information from the user home network 5. After performing mutual authentication with the user home network 5, the user management section 18 converts the temporary key Ktemp to a shared temporary key Ktemp, encrypts a distribution key Kd from the key server 14 by use of the shared temporary key Ktemp, and transmits it to the user home network 5. After decrypting the received distribution key Kd by use of the shared temporary key Ktemp, the user home network 5 updates the distribution key Kd if necessary. Further, the user home network 5 encrypts charging information, a handling policy, and other data by use of the shared temporary key Ktemp and transmits them to the EMD service center 1. The user management section 18 receives the encrypted data. After decrypting the received charging information, handling policy, and other data by use of the shared temporary key Ktemp, the user management section 18 transmits them to the historical-data management section 15 and the charge billing section 19. When the historical-data management section 15 judges that settlement must be executed, the historical-data management section 15 transmits the received charging information to the

profit-distribution section 16 and transmits the received charging information, handling policy, and other data to the charge billing section 19. With reference to the profit-distribution database and the discount table, the profit-distribution section 16 calculates amounts to be charged to and amounts to be paid to the content provider 2, the service provider 3, and the EMD service center 1, through processing which will be described later with reference to FIG. 57. The charge billing section 19 calculates an amount to be charged to each user on the basis of the user's usage-fee table, and transmits the information to the treasury section 20. The treasury section 20 communicates with an unillustrated outside bank or the like to thereby perform settlement processing. At this time, when information indicating user's nonpayment of fee or any other fact is present, such information is transmitted from the charge billing section 19 and the user management section 18 and is referred to during subsequent processing for user registration or processing for transmission of distribution keys Kd.

[0095] FIG. 32 shows an operation of the EMD service center 1 for profit distribution processing. The historical-data management section 15 transmits to the profit-distribution section 16 charging information indicative of past use of content by a user, a handling policy, and price data. On the basis of these information items, the profit-distribution section 16 calculates respective profits of the content provider 2, the service provider 3, and the EMD service

center 1 and transmits the results of calculation to the service-provider management section 11, the content-provider management section 12, the treasury section 20, and the copyright management section 13. The treasury section 20 communicates with the unillustrated outside bank or the like to thereby perform setting processing. The service-provider management section 11 transmits to the service provider 3 information regarding the profit of the service provider 3. The content-provider management section 12 transmits to the content provider 2 information regarding the profit of the content provider 2. The auditor section 21 audits accuracy of the charging information, price information, and handling policy supplied from the apparatus of the user home network 5.

[0096] FIG. 33 shows an operation of the EMD service center 1 for transmitting to JASRAC information regarding past use of content by a user. The historical-data management section 15 transmits to the copyright management section 13 and the profit-distribution section 16 charging information indicative of past use of the content by the user. With reference to the profit-distribution database and the discount table, the profit-distribution section 16 calculates an amount to be charged to and an amount to be paid to JASRAC, and transmits that information to the treasury section 20, through processing which will be described later with reference to FIG. 57. The treasury section 20 communicates with the unillustrated outside bank or the like to thereby perform settlement processing. The copyright management

section 13 transmits to JASRAC a record of use of the content by the user.

[0097] Next, processing performed by the EMD system will be described. FIG. 34 is a flowchart used for describing the processing performed by the system in order to distribute and reproduce content. In step S11, the content-provider management section 12 of the EMD service center 1 transmits distribution keys Kd to the content provider 2; and the content provider 2 receives them. The details of this processing will be described later with reference to the flowchart of FIG. 36. In step S12, a user operates an apparatus (e.g., the receiver 51 of FIG. 10) of the user home network 5 in order to register the apparatus in the user management section 18 of the EMD service center 1. The details of this registration processing will be described later with reference to the flowchart of FIG. 40. In step S13, as shown in FIGS. 37 to 39, the user management section 18 of the EMD service center 1 transmits distribution keys Kd to the apparatus of the user home network 5 after mutual authentication. The user home network 5 receives the keys. The details of this processing will be described later with reference to the flowchart of FIG. 48.

[0098] In step S14, the secure container creation section 38 of the content provider 2 transmits a content-provider secure container to the service provider 3. The details of this transmission processing will be described later with reference to the flowchart of FIG. 50. In step S15, in

response to a request from the user home network 5, the secure container creation section 44 of the service provider 3 transmits a service-provider secure container to the user home network 5 via the network 4. The details of this transmission processing will be described later with reference to the flowchart of FIG. 52. In step S16, the charging processing module 72 of the user home network 5 performs charging processing. The details of this charging processing will be described later with reference to the flowchart of FIG. 54. In step S17, the user reproduces the content on the apparatus of the user home network 5. The details of this reproduction processing will be described later with reference to the flowchart of FIG. 55.

[0099] Processing performed by the content provider 2 in order to encrypt and transmit a handling policy is shown by the flowchart of FIG. 35. In step S21, the content-provider management section 12 of the EMD service center 1 transmits distribution keys Kd to the content provider 2. In step S22, the service-provider management section 11 of the EMD service center 1 transmits distribution keys Kd to the service provider 3. Processing performed in subsequent steps S23 to S28 is similar to that performed in steps S12 to S17 of FIG. 24, and hence repeated description is omitted.

[0100] FIG. 36 is a flowchart used for describing the details of processing corresponds to step S11 of FIG. 34 and step S21 of FIG. 35. In this processing, the EMD service center 1 transmits distribution keys Kd to the content

provider 2, and the content provider 2 receives them. In step S31, the mutual authentication section 17 of the EMD service center 1 mutually authenticates with the mutual authentication section 39 of the content provider 2. The details of this mutual authentication processing will be described later with reference to the flowchart of FIG. 37. When, through the mutual authentication processing, the content provider 2 has been confirmed to be an authorized provider, in step S32 the encryption section 34 and the encryption section 36 of the content provider 2 receive the distribution keys Kd transmitted from the content-provider management section 12 of the EMD service center 1. In step S33, the encryption section 34 of the content provider 2 stores the received distribution keys Kd.

[0101] As described above, the content provider 2 receives the distribution keys Kd from the EMD service center 1. Similarly, in an example case in which processing of the flowchart shown in FIG. 35 is performed, not only the content provider 2 but also the service provider 3 receives the distribution keys Kd from the EMD service center 1, through processing similar to that shown in FIG. 36.

[0102] Next, the mutual authentication processing, which is performed in step S31 of FIG. 36 in order to confirm that so-called disguisement is not present, will be described with reference to three example cases; i.e., a case in which a single common key is used (FIG. 37), a case in which two common keys are used (FIG. 38), and a case in which a public

key cryptosystem is used (FIG. 39).

[0103] FIG. 37 is a flowchart showing mutual authentication operation which the mutual authentication section 39 of the content provider 2 and the mutual authentication section 17 of the EMD service center 1 perform while using a single common key of DES, which is a common key cryptosystem. In step S41, the mutual authentication section 39 of the content provider 2 generates a random number R1 of 64 bits (the random-number generation section 35 may generate the random number). In step S42, the mutual authentication section 39 of the content provider 2 encrypts the random number R1 by use of a previously stored common key Kc, in accordance with the DES (the encryption section 36 may perform this encryption). In step S43, the mutual authentication section 39 of the content provider 2 transmits the encrypted random number R1 to the mutual authentication section 17 of the EMD service center 1.

[0104] In step S44, the mutual authentication section 17 of the EMD service center 1 decrypts the received random number R1 by use of the previously stored common key Kc. In step S45, the mutual authentication section 17 of the EMD service center 1 generates a random number R2 of 32 bits. In step S46, the mutual authentication section 17 of the EMD service center 1 replaces lower 32 bits of the decrypted 64-bit random number R1 with the random number R2 to thereby generate a concatenated number $R1_H||R2$. Here, Ri_H represents the upper bits of Ri, and A||B represents a concatenation of

A and B (where B having m bits is joined to a lower portion of A having n bits to thereby obtain a number of (n+m) bits). In step S47, the mutual authentication section 17 of the EMD service center 1 encrypts the concatenated number $R1_H||R2$ by use of the common key Kc in accordance with the DES. In step S48, the mutual authentication section 17 of the EMD service center 1 transmits the encrypted $R1_H||R2$ to the content provider 2.

[0105] In step S49, the mutual authentication section 39 of the content provider 2 decrypts the received $R1_H||R2$ by use of the common key Kc. In step S50, the mutual authentication section 39 of the content provider 2 investigates the upper 32 bits $R1_H$ of the decrypted concatenated number $R1_H||R2$ and authenticates that the EMD service center 1 is an authorized center, when the upper 32 bits $R1_H$ coincide with the upper 32 bits $R1_H$ of the random number R1 generated in step S41. When the generated random number $R1_H$ does not coincide with the received $R1_H$, the processing is ended. When they coincide with each other, in step S51, the mutual authentication section 39 of the content provider 2 generates a random number R3 of 32 bits. In step S52, the mutual authentication section 39 of the content provider 2 generates a concatenated number R2||R3, while using the received and decrypted 32-bit random number as an upper half of the concatenated number and the generated random number R3 as a lower half of the concatenated number. In step S53, the mutual authentication section 39 of the content provider 2 encrypts the

concatenated number R2||R3 by use of the common key Ks in accordance with the DES. In step S54, the mutual authentication section 39 of the content provider 2 transmits the encrypted concatenation number R2||R3 to the mutual authentication section 17 of the EMD service center 1.

[0106] In step S55, the mutual authentication section 17 of the EMD service center 1 decrypts the received concatenated number R2||R3 by use of the common key Kc. In step S56, the mutual authentication section 17 of the EMD service center 1 investigates the upper 32 bits of the decrypted concatenated number R2||R3 and authenticates that the content provider 2 is an authorized provider, when the upper 32 bits coincide with the random number R2. When the upper 32 bits do not coincide with the random number R2, the content provider 2 is judged to be an unauthorized provider, and the processing is ended.

[0107] FIG. 38 is a flowchart showing mutual authentication operation which the mutual authentication section 39 of the content provider 2 and the mutual authentication section 17 of the EMD service center 1 perform while using two common keys Kc1 and Kc2 in accordance with DES, which is a common key cryptosystem. In step S61, the mutual authentication section 39 of the content provider 2 generates a random number R1 of 64 bits. In step S62, the mutual authentication section 39 of the content provider 2 encrypts the random number R1 by use of a previously stored common key Kc1 in accordance with the DES. In step S63, the mutual

authentication section 39 of the content provider 2 transmits the encrypted random number R1 to the EMD service center 1.

[0108] In step S64, the mutual authentication section 17 of the EMD service center 1 decrypts the received random number R1 by use of the previously stored common key Kc1. In step S65, the mutual authentication section 17 of the EMD service center 1 encrypts the random number R1 by use of a previously stored common key Kc2. In step S66, the mutual authentication section 17 of the EMD service center 1 generates a random number R2 of 64 bits. In step S67, the mutual authentication section 17 of the EMD service center 1 encrypts the random number R2 by use of the common key Kc2. In step S68, the mutual authentication section 17 of the EMD service center 1 transmits the encrypted random numbers R1 and R2 to the mutual authentication section 39 of the content provider 2.

[0109] In step S69, the mutual authentication section 39 of the content provider 2 decrypts the received random numbers R1 and R2 by use of the previously stored common key Kc2. In step S70, the mutual authentication section 39 of the content provider 2 investigates the decrypted random number R1 and authenticates that the EMD service center 1 is an authorized center, when the decrypted random number R1 coincides with the random number R1 generated in step S61 (random number R1 before being subjected to encryption). When they do not coincide with each other, the EMD service center 1 is judged to be an unauthorized center, and the processing is ended.

In step S71, the mutual authentication section 39 of the content provider 2 encrypts with the common key Kc1 the random number R2 obtained through decryption. In step S72, the mutual authentication section 39 of the content provider 2 transmits the encrypted random number R2 to the EMD service center 1.

[0110] In step S73, the mutual authentication section 17 of the EMD service center 1 decrypts the received random number R2 by use of the common key Kc1. In step S74, the mutual authentication section 17 of the EMD service center 1 authenticates that the content provider 2 is an authorized provider, when the decrypted random number R2 coincides with the random number R2 generated in step S66 (random number R2 before being subjected to encryption). When they do not coincide with each other, the content provider 2 is judged to be an unauthorized provider, and the processing is ended.

[0111] FIG. 39 is a flowchart showing mutual authentication operation performed by the mutual authentication section 39 of the content provider 2 and the mutual authentication section 17 of the EMD service center 1 while using an elliptic-curve cryptosystem of 160-bit length, which is a public key cryptosystem. In step S81, the mutual authentication section 39 of the content provider 2 generates a random number R1 of 64 bits. In step S82, the mutual authentication section 39 of the content provider 2 transmits to the mutual authentication section 17 of the EMD service center 1 the random number R1 and a certificate which has

been obtained in advance from an authentication office and which includes a public key Kpcp of the content provider 2.

[0112] In step S83, the mutual authentication section 17 of the EMD service center 1 decrypts the signature of the received certificate (having been encrypted by use of a private key Ksca of the authentication office) by use of a public key Kpca of the authentication office which has been obtained in advance, to thereby extract hash values of the public key Kpcp of the content provider 2 and the name of the content provider 2. The mutual authentication section 17 of the EMD service center 1 extracts the public key Kpcp of the content provider 2 and the name of the content provider 2, which are stored in the form of plain text. If the certificate is a proper one issued by the authentication office, decryption of the signature of the certificate is possible; and the hash values of the public key Kpcp of the content provider 2 and the name of the content provider 2 coincide with hash values obtained as a result of applying a hash function to the public key Kpcp of the content provider 2 and the name of the content provider 2 which are stored in the certificate in the form of plain text. Thus, the public key Kpcp is authenticated to be an authorized one and not to have been subjected to tampering. When the signature cannot be decrypted or when the hash values extracted from the signature do not coincide with those obtained by use of a hash function, this means that the public key Kpcp is not an authorized public key, or the content provider 2 is not an

authorized provider. In this case, the processing is ended.

[0113] When a proper authentication result is obtained, in step S84, the mutual authentication section 17 of the EMD service center 1 generates a random number R2 of 64 bits. In step S85, the mutual authentication section 17 of the EMD service center 1 generates a concatenated number R1||R2 of the random numbers R1 and R2. In step S86, the mutual authentication section 17 of the EMD service center 1 encrypts the concatenated number R1||R2 by use of the private key Ksesc of the EMD service center 1. In step S87, the mutual authentication section 17 of the EMD service center 1 encrypts the concatenated number R1||R2 by use of the public key Kpcp of the content provider 2 obtained in step S83. In step S88, the mutual authentication section 17 of the EMD service center 1 transmits to the mutual authentication section 39 of the content provider 2 the concatenated number R1||R2 encrypted by use of the private key Ksesc, the concatenated number R1||R2 encrypted by use of the public key Kpcp, and a certificate including the public key Kpesc of the EMD service center 1 (which has been obtained in advance from the authentication office).

[0114] In step S89, the mutual authentication section 39 of the content provider 2 decrypts the signature of the received certificate by use of the previously obtained public key Kpca of the authentication office; and when the signature is correct, the mutual authentication section 39 extracts the public key Kpesc from the certificate. Since the processing

in this case is similar to that in step S83, its repeated description is omitted. In step S90, the mutual authentication section 39 of the content provider 2 decrypts the concatenated number R1||R2 having been encrypted by use of the private key Ksesc of the EMD service center 1, by use of the public key Kpesc obtained in step S89. In step S91, the mutual authentication section 39 of the content provider 2 decrypts the concatenated number R1||R2 having been encrypted by use of the public key Kpcp of the content provider 2, by use of the private key Kscp of the content provider 2. In step S92, the mutual authentication section 39 of the content provider 2 compares the concatenated number R1||R2 decrypted in step S90 and that decrypted in step S91. When they coincide with each other, the mutual authentication section 39 authenticates that the EMD service center 1 is an authorized one. When they do not coincide with each other, the mutual authentication section 39 judges that the EMD service center 1 is not an authorized one, and ends the processing.

[0115] When a proper authentication result is obtained, in step S93, the mutual authentication section 39 of the content provider 2 generates a random number R3 of 64 bits. In step S94, the mutual authentication section 39 of the content provider 2 generates a concatenated number R2||R3 of the generated random number R3 and the random number R2 obtained in step S90. In step S95, the mutual authentication section 39 of the content provider 2 encrypts the concatenated number

R2||R3 by use of the public key Kpesc obtained in step S89. In step 96, the mutual authentication section 39 of the content provider 2 transmits the encrypted, concatenated number R2||R3 to the mutual authentication section 17 of the EMD service center 1.

[0116] In step S97, the mutual authentication section 17 of the EMD service center 1 decrypts the encrypted, concatenated number R2||R3 by use of the private key Ksesc of the EMD service center 1. In step S98, the mutual authentication section 17 of the EMD service center 1 authenticates that the content provider 2 is an authorized provider, when the decrypted random number R2 coincides with the random number R2 generated in step S84 (random number R2 before being subjected to encryption). When they do not coincide with each other, the mutual authentication section 17 judges that the content provider 2 is not an authorized provider, and ends the processing.

[0117] As described above, the mutual authentication section 17 of the EMD service center 1 and the mutual authentication section 39 of the content provider 2 authenticate each other. Random numbers used in the mutual authentication are each used as a temporary key Ktemp, which is effective only in processing subsequent to the mutual authentication.

[0118] FIG. 40 is a flowchart used for describing the details of processing corresponding to step S12 of FIG. 34 and step S23 of FIG. 35. In this processing, the receiver 51 performs registration in the user management section 18 of the EMD

service center 1. In step S101, on the basis of output from the IC-card interface 64, the SAM 62 of the receiver 51 judges whether the IC card 55 for backup is attached to the receiver 51. When the IC card 55 for backup has been attached to the receiver 51 (e.g., a case in which the receiver 51 is replaced with a new receiver 51, and the data contained in the previous receiver 51 are stored in the IC card 55 in order to transfer the data of the previous receiver 51 to the new receiver 51), the SAM 62 proceeds to step S102 in order to read backup data stored in the IC card 55. The details of this processing will be described later with reference to the flowchart of FIG. 45. Needless to say, in order to enable this read processing, the backup data must be stored in the IC card 55 beforehand. This backup processing will be described later with reference to FIG. 43.

[0119] When in step S101 the IC card 55 is judged not to be attached to the receiver 51, the SAM 62 skips step S102 and proceeds to step S103. In step S103, the mutual authentication module 71 of the SAM 62 mutually authenticates with the mutual authentication section 17 of the EMD service center 1, and the SAM 62 transmits a certificate to the user management section 18 of the EMD service center 1. Since this authentication processing is similar to that having been described with reference to FIGS. 37 to 39, its repeated description is omitted here. The certificate that the SAM 62 transmits to the user management section 18 of the EMD service center 1 in step S103 includes data shown in FIG. 41.

The certificate transmitted by the SAM 62 has a configuration substantially the same as that of the content provider 2 shown in FIG. 14. However, the certificate transmitted by the SAM 62 further contains data indicating whether the SAM 62 belongs to another SAM. In step S104, the SAM 62 transmits, via the communication section 61 to the user management section 18 of the EMD service center 1, information regarding a settlement institution such as a bank of the user, which information has been encrypted by use of the temporary key Ktemp.

[0120] In step S105, on the basis of the received ID of the SAM 62, the user management section 18 of the EMD service center 1 searches the user-registration database shown in FIG. 7. In step S106, the user management section 18 of the EMD service center 1 judges whether a SAM 62 having the received ID can be registered. When the SAM 62 can be registered, the user management section 18 proceeds to step S107 in order to judge whether registration of the SAM 62 is new. When it is judged in step S107 that the registration of the SAM 62 is not a new registration, the user management section 18 proceeds to step S108.

[0121] In step S108, the user management section 18 of the EMD service center 1 executes processing for update registration in order to search the user-registration data base on the basis of the received Id and to make a registration list. This registration list has a configuration as shown in FIG. 42. For each of the IDs of

SAMs of apparatuses, this registration list includes a registration denial flag indicating whether the user management section 18 of the EMD service center 1 has denied registration; a status flag which is used in a case in which an SAM depends on another SAM and which shows conditions for use of a content key Kco; a condition flag indicating whether the SAM depends on another SAM; and a signature. The signature has been obtained through encryption, with the private key Ksesc of the EMD service center 1, of a hash value generated through application of a hash function to the registration denial flag, the status flag, and the condition flag.

[0122] The SAM of each apparatus has a 64-bit ID unique to the apparatus (indicated by hexadecimal numbers in FIG. 42). When the registration denial flag is "1," this indicates that the user management section 18 of the EMD service center 1 has registered an apparatus having a corresponding ID. When the registration denial flag is "0," this indicates that the user management section 18 of the EMD service center 1 has denied registration of an apparatus having a corresponding ID.

[0123] When the MSB (Most Significant Bit) of the status flag is "1," this indicates that a child apparatus having a corresponding ID (e.g., the recorder 53) can receive a content key Kco from a parent apparatus (e.g., the receiver 51) on which the child apparatus depends. When the MSB of the status flag is "0," this indicates that a child apparatus having a corresponding ID cannot receive a content key Kco

from a parent apparatus on which the child apparatus depends. When the second bit of the status flag as counted from the MSB is "1," this indicates that a child apparatus having a corresponding ID can receive from a parent apparatus a content key Kco encrypted by use of a save key Ksave of the parent apparatus. When the third bit of the status flag as counted from the MSB is "1," this indicates that a child apparatus having a corresponding ID can receive from a parent apparatus a content key Kco encrypted by use of a distribution key Kd. When the LSB (Least Significant Bit) of the status flag is "1," this indicates that a parent apparatus on which a child apparatus having a corresponding ID depends purchases a content key Kco encrypted by use of a distribution key Kd, encrypts the content key Kco by use of a temporary key Ktemp, and passes the encrypted content key Kco to the child apparatus.

[0124] When the condition flag is "0," this indicates that an apparatus having a corresponding ID can communicate directly with the user management section 18 of the EMD service center 1 (i.e., this indicates that the apparatus having a corresponding ID is a parent apparatus such as the receiver 51). When the condition flag is "1," this indicates that an apparatus having a corresponding ID cannot communicate directly with the user management section 18 of the EMD service center 1 (i.e., this indicates that the apparatus having a corresponding ID is a child apparatus such as the recorder 53). When the condition flag is "0," the

status flag is set to "0000" at all times.

[0125] In step S109, the user management section 18 of the EMD service center 1 transmits to the SAM 62 of the receiver 51 a distribution key Kd which has been supplied from the key server 14 and encrypted by use of a temporary key Ktemp supplied from the mutual authentication section 17. In step S110, the SAM 62 of the receiver 51 decrypts the received distribution key Kd by use of the temporary key Ktemp and stores it in the storage module 73.

[0126] In step S111, the user management section 18 of the EMD service center 1 transmits to the SAM 62 of the receiver 51 the registration list encrypted by use of the temporary key Ktemp. In step S112, the SAM 62 of the receiver 51 decrypts the received registration list by use of the temporary key Ktemp and stores it in the storage module 73. Subsequently, the processing is ended.

[0127] When it is judged in step S107 that the registration of the SAM 62 is a new registration, the user management section 18 of the EMD service center 1 proceeds to step S114 to perform processing for new registration and produce a registration list. Subsequently, the user management section 18 proceeds to step S109.

[0128] When it is judged in step S106 that registration of a SAM having the received ID is impossible, the user management section 18 of the EMD service center 1 proceeds to step S113 to produce a registration list for registration denial. Subsequently, the user management section 18 proceeds to step

S111.

[0129] In the above-described manner, the receiver 51 is registered in the EMD service center 1.

[0130] Next, with reference to the flowchart of FIG. 43, there will be described the details of processing for storing in the IC card 55 predetermined data, such as a distribution key, which are stored in the storage module 73 of the receiver 51 having been used up to the present. In step S121, the mutual authentication module 71 of the SAM 62 mutually authenticates with the mutual authentication module 80 of the IC card 55. Since this mutual authentication is the same as that described with reference to FIGS. 37 to 39, repeated description is omitted here. In step S122, the random-number generation unit 92 of the SAM 62 generates a random number used as a backup key Kic. In step S123, the encryption unit 93 of the SAM 62 encrypts the ID number of the SAM, the save key Ksave, and the ID of the HDD 52, which are stored in the storage module 73, by use of the backup key Kic. In step S124, the encryption unit 93 of the SAM 62 encrypts the backup key Kic by use of the public key Kpesc of the EMD service center 1 (the SAM 62 has already obtained the public key Kpesc of the EMD service center 1 during authentication processing performed with the EMD service center 1 (step S89 in FIG. 39)). In step S125, the SAM 62 of the receiver 51 transmits, via the IC-card interface 64 to the IC card 55, the encrypted ID number of the SAM, the encrypted save key Ksave, the encrypted ID of the HDD 52, and the encrypted

backup key Kic, to thereby store them in the storage module 81.

[0131] As described above, the ID number of the SAM, the save key Ksave, and the ID of the HDD 52, which are stored in the storage module 73 of the SAM 62, are encrypted by use of the backup key Kic, and stored in the storage module 81 of the IC card 55, together with the backup key Kic, which is encrypted by use of the public key Kpesc of the EMD service center 1.

[0132] With reference to the flowchart of FIG. 44, there will be described the details of other processing for storing in the IC card 55 predetermined data, such as a distribution key, which are stored in the storage module 73 of the receiver 51 having been used up to the present. In step 131, the mutual authentication module 71 of the SAM 62 mutually authenticates with the mutual authentication module 80 of the IC card 55. In step S132, the encryption unit 93 of the SAM 62 encrypts the ID number of the SAM, the save key Ksave, and the ID of the HDD 52, which are stored in the storage module 73, by use of the public key Kpesc of the EMD service center 1. In step S133, the SAM 62 of the receiver 51 transmits, via the IC-card interface 64 to the IC card 55, the encrypted ID number of the SAM, the encrypted save key Ksave, and the encrypted ID of the HDD 52, to thereby store them in the storage module 81.

[0133] The processing shown in FIG. 44, which is simpler than that shown in FIG. 43, enables the ID number of the SAM,

the save key Ksave, and the ID of the HDD 52 to be stored in the storage module 81 of the IC card 55 after being encrypted by use of the public key Kpesc of the EMD service center 1.

[0134] As described above, the backup data stored in the IC card 55 are read into the new receiver 51 by the processing in step S102 of FIG. 40. FIG. 45 is a flowchart used for describing processing for reading the backup data which have been stored in the IC card 55 by the processing shown in FIG. 43. In step 141, the mutual authentication module 71 of the SAM 62 of the new receiver 51 mutually authenticates with the mutual authentication module 80 of the IC card 55. Since this mutual authentication is the same as that described with reference to FIGS. 37 to 39, repeated description is omitted here.

[0135] In step S142, the SAM 62 reads via the IC-card interface 64 from the storage module 81 data which was stored in the storage module 73 of the previous receiver 51 and encrypted by use of the backup key Kic (backup data of the ID number of the SAM, the save key Ksave, and the ID of the HDD 52), and the backup key Kic encrypted by use of the public key Kpesc of the EMD service center 1. In step S143, the mutual authentication module 71 of the SAM 62 mutually authenticates with the mutual authentication section 17 of the EMD service center 1 via the communication section 61. Since this mutual authentication is the same as that described with reference to FIGS. 37 to 39, repeated description is omitted here. In step S144, the SAM 62

transmits, via the communication section to the user management section 18 of the EMD service center 1, the data of the storage module 73 encrypted by use of the backup key Kic, as well as the backup key Kic encrypted by use of the public key Kpesc of the EMD service center 1.

[0136] In step S145, the user management section 18 of the EMD service center 1 decrypts the received backup key Kic by use of the private key Ksesc of the EMD service center 1. In step S146, the user management section 18 of the EMD service center 1 decrypts the received backup data by use of the backup key Kic. In step S147, the user management section 18 of the EMD service center 1 encrypts the decrypted backup data by use of the temporary key Ktemp supplied from the mutual authentication section 17. In step S148, the user management section 18 of the EMD service center 1 transmits to the communication section 61 of the user home network 51 the backup data encrypted by use of the temporary key Ktemp.

[0137] In step S149, the communication section 61 of the user home network 51 transmits to the SAM 62 the data received from the user management section 18 of the EMD service center 1. The SAM 62 decrypts the data and then stores them in the storage module 73. In step S150, the user management section 18 of the EMD service center 1 modifies the data in the user-registration database (FIG. 7) corresponding to the ID of the SAM 62 of the previous apparatus from which data was transferred to the IC card 55, such that the modified data indicate un-registerable.

[0138] As described above, the new receiver 51 reads the backup data from the IC card 55.

[0139] With reference to the flowchart shown in FIG. 46, there will be described processing for reading the backup data which have been stored in the IC card 55 by the processing shown in FIG. 44. In step S161, the mutual authentication module 71 of the SAM 62 of the new receiver 51 mutually authenticates with the mutual authentication module 80 of the IC card 55. Since this mutual authentication is the same as that described with reference to FIGS. 37 to 39, repeated description is omitted here. In step S162, the SAM 62 reads via the IC-card interface 64 data which was stored in the storage module 73 of the previous receiver 51 and encrypted by use of the public key Kpesc of the EMD service center 1 (backup data of the ID number of the SAM, the save key Ksave, and the ID of the HDD 52).

[0140] In step S163, the mutual authentication module 71 of the SAM 62 mutually authenticates with the mutual authentication section 17 of the EMD service center 1 via the communication section 61. Since this mutual authentication is the same as that described with reference to FIGS. 37 to 39, repeated description is omitted here. In step S164, the SAM 62 transmits, via the communication section 61 to the user management section 18 of the EMD service center 1, the data of the storage module 73 encrypted by use of the public key Kpesc of the EMD service center 1.

[0141] In step S165, the user management section 18 of the

EMD service center 1 decrypts the data of the storage module 73 by use of the private key Ksesc of the EMD service center 1. In step S166, the user management section 18 of the EMD service center 1 encrypts the decrypted backup data by use of the temporary key Ktemp supplied from the mutual authentication section 17. In step S167, the user management section 18 of the EMD service center 1 transmits to the communication section 61 of the user home network 51 the backup data encrypted by use of the temporary key Ktemp.

[0142] In step S168, the communication section 61 of the receiver 51 transmits to the SAM 62 the data received from the user management section 18 of the EMD service center 1. The SAM 62 decrypts the data and then stores them in the storage module 73. In step S169, the user management section 18 of the EMD service center 1 modifies the data in the user-registration database (FIG. 7) corresponding to the ID of the SAM 62 of the previous apparatus from which data was transferred to the IC card 55, such that the modified data indicate un-registerable.

[0143] As described above, when the backup is performed by use of the processing shown in FIG. 44, the new receiver 51 reads the backup data from the IC card 55 through the processing shown in FIG. 46.

[0144] When the receiver 51 registers itself (when the receiver 51 perform processing corresponding to step S12 of FIG. 34), the receiver 51 performs the processing shown in the flowchart of FIG. 40. When the receiver 51 registers the

recorder 53 depending on the receiver 51 in the EMD service center 1, the receiver 51 performs the processing shown in the flowchart of FIG. 47. In step S181, the SAM 62 of the receiver 51 writes the ID of the recorder 53 into the registration list stored in the storage module 73. In step S182, the mutual authentication module 71 of the receiver 51 mutually authenticates with the mutual authentication section 17 of the EMD service center 1. Since this mutual authentication is the same as that described with reference to FIGS. 37 to 39, repeated description is omitted here.

[0145] In step S183, on the basis of the ID of the receiver 51 (the ID of the SAM 62 contained in the certificate of the SAM 62 shown in FIG. 41), the user management section 18 of the EMD service center 1 searches the user-registration database and judges whether the receiver 51 is un-registerable. When the receiver 51 is judged not to be un-registerable, the processing proceeds to step S184. In step 184, the SAM 62 of the receiver 51 encrypts, by use of the temporary key Kd, the version of the distribution key Kd, charging information (stored by the processing in step S337 of the flowchart shown in FIG. 54, which will be described later), and the registration list, which are stored in the storage module 73. Further, the SAM 62 encrypts the handling policy stored in the HDD 52 by use of the temporary key Kd. Subsequently, the SAM 62 transmits via the communication section 61 to the user management section 18 of the EMD service center 1 the version of the distribution key Kd, the

charging information, and the registration list, which are stored in the storage module 73, as well as the handling policy stored in the HDD 52. In step S185, the user management section 18 of the EMD service center 1 decrypts the received data and processes the charging information. Subsequently, the user management section 18 updates the data portion (e.g., the registration denial flag and the status flag) which relates to the recorder 53 and which is contained in the registration list received from the receiver 51. The user management section 18 then attaches to the updated registration list a signature corresponding to the data corresponding to the receiver 51.

[0146] In step S186, the user management section 18 of the EMD service center 1 judges whether the version of the distribution key Kd which the receiver 51 holds is the latest. When the version of the distribution key Kd held by the receiver 51 is judged to be the latest, in step S187, the user management section 18 transmits to the receiver 51 the updated registration list and a charging-information receipt message, which have been encrypted by use of the temporary key Kd. The receiver 51 receives the updated registration list and the charging-information receipt message, decrypts them, and stores them. In step S188, the receiver 51 erases the charging information stored in the storage module 73, and replaces the stored registration list with the registration list received from the user management section 18 of the EMD service center 1 in step S187. Subsequently, the processing

proceeds to step S191.

[0147] When it is judged in step S186 that the version of the distribution key Kd held by the receiver 51 is not the latest, in step S189, the user management section 18 of the EMD service center 1 transmits to the receiver 51 a distribution key of the latest version, the updated registration list, and the charging-information receipt message, which have been encrypted by use of the temporary key Kd. The receiver 51 receives the distribution key of the latest version, the updated registration list, and the charging information receipt message, decrypts them, and stores them. In step S190, the receiver 51 erases the charging information stored in the storage module 73, replaces the stored registration list with the registration list received from the user management section 18 of the EMD service center 1 in step S189, and replaces the previous distribution key Kd with the distribution key of the latest version. Subsequently, the processing proceeds to step S191.

[0148] In step S191, with reference to the updated registration list, the SAM 62 of the receiver 51 judges whether the recorder 53 is un-registerable. When the recorder 53 is judged not to be un-registerable, in step S192, the receiver 51 and the recorder 53 mutually authenticate and share the temporary key Ktemp. Since this authentication processing is similar to that having been described with reference to FIGS. 37 to 39, repeated description is omitted here. In step S193, the receiver 51 transmits to the

recorder 53 a registration completion message and the distribution key Kd, which have been encrypted by use of the temporary key Kd. The recorder 53 receives the registration completion message and the distribution key Kd, and decrypts them. In step S194, the recorder 53 updates the distribution key Kd, after which the processing ends.

[0149] The processing ends when it is judged in step S183 that the receiver 51 is un-registerable, or when it is judged in step S191 that the recorder 53 is un-registerable.

[0150] As described above, the recorder 53 depending on the receiver 51 is registered in the EMD service center 1 via the receiver 51.

[0151] FIG. 48 is a flowchart showing the details of the processing which is performed in step S13 of FIG. 34 in order to enable the receiver 51 to receive a distribution key Kd which is transmitted from the EMD service center 1 to the receiver 51. In step S201, the mutual authentication module 71 of the receiver 51 mutually authenticates with the mutual authentication section 17 of the EMD service center 1. Since this authentication processing is similar to that having been described with reference to FIGS. 37 to 39, repeated description is omitted here. In step S202, the SAM 62 of the receiver 51 transmits a certificate to the user management section 18 of the EMD service center 1; and the user management section 18 of the EMD service center 1 receives the certificate. Since the processing in steps S203 to S210 is the same as that in steps S183 to S190 of FIG. 47,

repeated descriptions are omitted here.

[0152] As described above, the receiver 51 receives a distribution key Kd from the user management section 18 of the EMD service center 1 and transmits charging information of the receiver 51 to the user management section 18 of the EMD service center 1.

[0153] Next, with reference to the flowchart of FIG. 49, there will be described the details of the processing which enables the recorder 53 depending on the receiver 51 to receive a distribution key Kd (when the status flag shown in FIG. 42 has a value indicating that the recorder 53 is permitted to receive a distribution key Kd). In step S221, the mutual authentication module 71 of the receiver 51 and an unillustrated mutual authentication module of the recorder 53 mutually authenticate. Since this authentication processing is similar to that having been described with reference to FIGS. 37 to 39, repeated description is omitted here.

[0154] In step S222, the receiver 51 judges whether the data of the recorder 53 are included in the registration list stored in the storage module 73 of the receiver 51. When it is judged that the data of the recorder 53 are included in the registration list stored in the storage module 73 of the receiver 51, in step S223, the receiver 51 judges whether the recorder 53 is un-registerable, with reference to the registration list stored in the storage module 73. When it is judged in step S223 that the recorder 53 is not un-registerable, in step S224, the SAM 66 of the recorder 53

encrypts, by use of the temporary key Ktemp, the version of the distribution key Kd stored in the internal storage module (which has been received from the receiver 51 in step S235 of FIG. 49, which will be described later) and charging information (which has been stored through processing corresponding step S337 of the processing corresponding to FIG. 54, which will be described later). Subsequently, the SAM 66 of the recorder 53 sends them to the SAM 62 of the receiver 51. The SAM 62 of the receiver 51 receives and decrypts the version of the distribution key Kd and the charging information.

[0155] In step S225, the mutual authentication module 71 of the receiver 51 mutually authenticates with the mutual authentication section 17 of the EMD service center 1 via the communication section 61. Since this authentication processing is similar to that having been described with reference to FIGS. 37 to 39, repeated description is omitted here. In step S226, on the basis of the ID of the receiver 51, the user management section 18 of the EMD service center 1 searches the user-registration database and judges whether the receiver 51 is un-registerable. When the receiver 51 is judged not to be un-registerable, processing proceeds to step S227. In step 227, the SAM 62 of the receiver 51 encrypts, by use of the temporary key Kd, the version of the distribution key Kd, the charging information, and the registration list, which are stored in the storage module 73. Further, the SAM 62 encrypts the handling policy stored in

the HDD 52 and the charging information of the recorder 53 by use of the temporary key Kd. Subsequently, the SAM 62 transmits these data to the user management section 18 of the EMD service center 1 via the communication section 61. In step S228, the user management section 18 of the EMD service center 1 decrypts the received data and processes the charging information. Subsequently, the user management section 18 updates the data portion (e.g., the registration denial flag and the status flag) which relates to the recorder 53 and which is contained in the registration list received from the receiver 51, as has been described in relation to FIG. 42. The user management section 18 then attaches to the updated registration list a signature corresponding to the data corresponding to the receiver 51.

[0156] Since the processing in steps S229 to S234 is the same as that in steps S186 to S191 of FIG. 47, repeated description is omitted here.

[0157] In step S234, with reference to the updated registration list, the SAM 62 of the receiver 51 judges whether the recorder 53 is un-registerable. When the recorder 53 is judged not to be un-registerable, in step S235, the receiver 51 transmits to the recorder 53 a charging-information receipt message and the distribution key Kd, which have been encrypted by use of the temporary key Kd. The recorder 53 receives the charging-information receipt message and the distribution key Kd, and decrypts them. In step S236, the SAM 66 of the recorder 53 erases the charging

information stored in the internal storage module, and replaces the stored distribution key Kd with the distribution key Kd of the latest version.

[0158] When it is judged in step S222 that the data of the recorder 53 are not included in the registration list stored in the storage module 73 of the receiver 51, in step S237, the processing shown in FIG. 47 for registering the recorder 53 is executed. Processing then proceeds to step S224.

[0159] The processing ends when it is judged in step S223 that the recorder 53 is un-registerable, when it is judged in step S226 that the receiver 51 is un-registerable, or when it is judged in step S234 that the recorder 53 is un-registerable.

[0160] As described above, the recorder 53 depending on the receiver 51 receives the distribution key Kd via the receiver 51.

[0161] Next, with reference to the flowchart of FIG. 50, there will be described the processing which corresponds to step S14 of FIG. 34 and which enables the content provider 2 to transmit a content-provider secure container to the service provider 3. In step S251, the watermark adding section 32 of the content provider 2 inserts into content supplied from the content server 31 a predetermined watermark indicating the content provider 2, and sends it to the compression section 33. In step S252, the compression section 33 of the content provider 2 compresses the content in which the watermark has been inserted, in accordance with

ATRAC2 or any other scheme and supplies the compressed content to the encryption section 34. In step S253, the random-number generation section 35 generates a random number which is used as a content key Kco, and outputs it to the encryption section 34. In step S254, the encryption section 34 of the content provider 2 encrypts the content——into which the watermark has been inserted and which has been compressed, by use the content key Kco and in accordance with a predetermined scheme such as DES.

[0162] In step S255, the encryption section 36 encrypts the content key Kco in accordance with a predetermined scheme such as DES and by use of the distribution key Kd which has been supplied from the EMD service center 1 through the processing in step S11 of FIG. 34. In step S256, the secure container creation section 38 of the content provider 2 applies a hash function to the encrypted content, the encrypted content key Kco, and the handling policy supplied from the policy storage section 37, in order to obtain a hash value, and then encrypts it by use of a private key Kscp of the content provider 2. Thus, a signature as shown in FIG. 13 is created. In step S257, the secure container creation section 38 of the content provider 2 creates a content-provider secure container as shown in FIG. 13, which includes the encrypted content, the encrypted content key Kco, and the handling policy supplied from the policy storage section 37, as well as the signature generated in step S256.

[0163] In step S258, the mutual authentication section 39 of

the content provider 2 mutually authenticates with the mutual authentication section 45 of the service provider 3. Since this mutual authentication is the same as that described with reference to FIGS. 37 to 39, repeated description is omitted here. In step S259, the secure container creation section 38 of the content provider 2 attaches to the content-provider secure container a certificate issued by the authentication office in advance and then transmits it to the service provider 3. Subsequently, the secure container creation section 38 ends the processing.

[0164] In the above-described manner, the content provider 2 transmits a content-provider secure container to the service provider 3.

[0165] Next, with reference to the flowchart of FIG. 51, there will be described the details of other processing which enables the content provider 2 to transmit a content-provider secure container to the service provider 3, wherein not only the content key Kco but also the handling policy is encrypted by use of the distribution key Kd. Since the processing in steps S271 to S274 is the same as that in steps S251 to S254 of FIG. 50, repeated description is omitted here. In step S275, the encryption section 36 of the content provider 2 encrypts the content key Kco and the handling policy supplied from the policy storage section 73, in accordance with a predetermined scheme such as DES and by use of the distribution key Kd which has been supplied from the EMD service center 1 through the processing in step S21 of FIG.

35.

[0166] In step S276, the secure container creation section 38 of the content provider 2 applies a hash function to the encrypted content, the encrypted content key Kco, and the encrypted handling policy in order to obtain a hash value, and then encrypts it by use of a private key Kscp of the content provider 2. Thus, a signature as shown in FIG. 25 is created. In step S277, the secure container creation section 38 of the content provider 2 creates a content-provider secure container as shown in FIG. 25, which includes the encrypted content, the encrypted content key Kco, and the encrypted handling policy, as well as the signature. The processing in step S278 is the same as that in step S258 of FIG. 50, and the processing in step S279 is the same as that in step S259 of FIG. 50. Therefore, repeated descriptions are omitted.

[0167] In the above-described manner, the content provider 2 transmits to the service provider 3 a content-provider secure container containing the encrypted handling policy.

[0168] Next, with reference to the flowchart of FIG. 52, there will be described the details of the processing which corresponds to step S15 of FIG. 34 and which enables the service provider 3 to transmit a service-provider secure container to the receiver 51. In step S291, the pricing section 42 of the service provider 3 checks the signature contained in the certificate which is attached to the content-provider secure container transmitted from the secure

container creation section 38 of the content provider 2. When the certificate has not been subjected to tampering, the pricing section 42 extracts the public key Kpcp of the content provider 2. Since the processing for checking the signature of the certificate is the same as that in step S83, repeated description is omitted here.

[0169] In step S292, the pricing section 42 of the service provider 3 decrypts, by use of the public key Kpcp of the content provider 2, the signature of the content-provider secure container transmitted from the secure container creation section 38 of the content provider 2, to thereby obtain a hash value. Subsequently, the pricing section 42 confirms that the thus-obtained hash value coincides with the hash value which is obtained through application of the hash function to the encrypted content, the encrypted content key Kco, and the handling policy, thereby confirming that the content-provider secure container has not been subjected to tampering. When it is found that the content-provider secure container has been subjected to tampering, the pricing section 42 ends the processing.

[0170] When the content-provider secure container has not been subjected to tampering, in step S293, the pricing section 42 of the service provider 3 extracts the handling policy from the content-provider secure container. In step S294, on the basis of the handling policy, the pricing section 42 of the service provider 3 produces price information, which has been described in relation to FIG. 17.

In step S295, the secure container creation section 44 of the service provider 3 produces a service-provider secure container as shown in FIG. 15. The service-provider secure container includes an encrypted content, an encrypted content key Kco, a handling policy, and price information, and a signature which is a value obtained through encryption, by use of its own private key Kssp, of a hash value which is obtained through application of a hash function to the encrypted content, the encrypted content key Kco, the handling policy, and the price information.

[0171] In step S296, the mutual authentication section 45 of the service provider 3 mutually authenticates with the mutual authentication module 71 of the receiver 51. Since this mutual authentication is the same as that described with reference to FIGS. 37 to 39, repeated description is omitted here. In step S297, the secure container creation section 44 of the service provider 3 transmits to the communication section 61 of the receiver 51 the service-provider secure container to which the certificate has been attached. Subsequently, the secure container creation section 44 ends the processing.

[0172] In the above-described manner, the service provider 3 transmits a service-provider secure container to the receiver 51.

[0173] Next, with reference to the flowchart of FIG. 53, there will be described the details of the processing which enables the service provider 3 to transmit a service-provider

secure container to the receiver 51, wherein the handling policy is encrypted by use of the distribution key Kd in the content provider 2, and the service provider 3 produces handling control information. Since processing in step S311 and processing in step S312 are the same as those in steps S291 and S292 of FIG. 52, repeated descriptions are omitted here. In step S313, the pricing section 42 of the service provider 3 decrypts the encrypted handling policy contained in the content-provider secure container. In step S314, on the basis of the handling policy, the pricing section 42 of the service provider 3 produces the handling control information which has been described in relation to FIG. 23. Since processing in step S315 through step S318 is the same as that in steps S294 through S297 of FIG. 52, repeated description is omitted.

[0174] As described above, the service provider 3 transmits to the receiver 51 a service-provider secure container containing the encrypted handling policy.

[0175] Next, with reference to the flowchart of FIG. 54, there will be described the processing which corresponds to step S16 of FIG. 34 and which enables the receiver 51 to perform charging processing after reception of a proper service-provider secure container. In step S331, the decryption/encryption module 74 of the receiver 51 judges whether the content key Kco can be decrypted by use of the distribution key Kd. When it is judged that the content key Kco cannot be decrypted by use of the distribution key Kd, in

step S332, the receiver 51 executes the processing for receiving the distribution key Kd, which has been described in relation to FIG. 48, and then proceeds to step S333. When it is judged in step S331 that the content key Kco can be decrypted by use of the distribution key Kd, the processing skips step S332 and proceeds to step S333. In step S333, the decryption unit 91 of the receiver 51 decrypts the content key Kco by use of the distribution key Kd, which has been stored in the storage module 73 through processing in step S13 of FIG. 34.

[0176] In step S334, the charging processing module 72 of the receiver 51 extracts the handling policy and the price information from the service-provider secure container and produces the charging information and the conditions-for-use information, which have been described with reference to FIGS. 19 and 20, respectively. In step S335, the charging processing module 72 of the receiver 51 judges whether the current charge is greater than the upper limit of charge, on the basis of the charging information stored in the storage module 73 and the charging information calculated in step S334. When the current charge is judged to be greater than the upper limit of charge, in step S336, the receiver 51 executes the processing for receiving the distribution key Kd, which has been described in relation to FIG. 48, to thereby obtain a new distribution key Kd. Subsequently, the receiver 51 proceeds to step S337. When it is judged in step S335 that the current charge is less than the upper limit of

charge, the receiver 51 skips steps 336 and proceeds to step S337.

[0177] In step S337, the charging processing module 72 of the receiver 51 stores the charging information in the storage module 73. In step S338, the charging processing module 72 of the receiver 51 stores in the HDD 52 the conditions-for-use information generated in step S334. In step S339, the SAM 62 of the receiver 51 registers in the HDD 52 the handling policy extracted from the service-provider secure container.

[0178] In step S340, the decryption/encryption module 74 of the receiver 51 applies the hash function to the conditions-for-use information to thereby calculate a hash value. In step S341, the storage module 73 of the receiver 51 stores the hash value of the conditions-for-use information. In the case in which the save key Ksave is not stored in the storage module 73, in step S342, the random-number generation unit 92 of the receiver 51 generates a random number serving as a save key Ksave. Subsequently, the receiver 51 proceeds to step S343. In the case in which the save key Ksave is stored in the storage module 73, the receiver 51 skips step S342 and proceeds to step S343.

[0179] In step S343, the encryption unit 93 of the receiver 51 encrypts the content key Kco by use of the save key Ksave. In step S344, the SAM 62 of the receiver 51 stores the encrypted content key Kco in the HDD 52. In the case in which the save key Ksave is not stored in the storage module

73, in step S345, the decryption/encryption module 74 of the receiver 51 stores the save key Ksave in the storage module 73. Subsequently, the receiver 51 ends the processing. In the case in which the save key Ksave is stored in the storage module 73, the receiver 51 skips step S345 and ends the processing.

[0180] In the above-described manner, the receiver 51 stores the charging information in the storage module 73, decrypts the content key Kco by use of the distribution key Kd, encrypts the content key Kco by use of the save key Ksave, and stores it in the HDD 52. The save key Ksave is stored in the storage module 73.

[0181] Through processing similar to the above-described processing, the recorder 53 stores the charging information in the storage module provided within the SAM 66, decrypts the content key Kco by use of the distribution key Kd, encrypts the content key Kco by use of the save key Ksave, and stores it in the HDD 52. The save key Ksave is stored in the storage module within the SAM 66.

[0182] With reference to the flowchart of FIG. 55, there will be described the processing which corresponds to step S17 of FIG. 34 and which enables the receiver 51 to reproduce content. In step S361, the decryption/encryption module 74 of the receiver 51 reads out of the HDD 52 the conditions-for-use information stored in step S338 of FIG. 54 and the encrypted content key Kco stored in step S344 of FIG. 54. In step S362, the decryption/encryption module 74 of the

receiver 51 applies the hash function to the conditions-for-use information to calculate a hash value.

[0183] In step S363, the decryption/encryption module 74 of the receiver 51 judges whether the hash value calculated in step S362 coincides with hash value which was stored in the storage module 73 in step S340 of FIG. 54. When the hash value calculated in step S362 is judged to coincide with hash value stored in the storage module 73, in step S364, the decryption/encryption module 74 of the receiver 51 updates predetermined information, such as a value indicating the number of times of use, contained in the conditions-for-use information. In step S365, the decryption/encryption module 74 of the receiver 51 applies the hash function to the updated conditions-for-use information to thereby obtain a hash value. In step S366, the storage module 73 of the receiver 51 stores the hash value of the conditions-for-use information calculated in step S365. In step S367, the decryption/encryption module 74 of the receiver 51 records the updated conditions-for-use information in the HDD 52.

[0184] In step S368, the mutual authentication module 71 of the SAM 62 and the mutual authentication module 75 of the extension section 63 mutually authenticate, and the SAM 62 and the extension section 63 store the temporary key Ktemp. Since this authentication processing is similar to that having been described with reference to FIGS. 37 to 39, repeated description is omitted here. The random number R1, R2, or R3 used in the mutual authentication is used as a

temporary key Ktemp. In step S369, by use of the save key Ksave stored in the storage module 73, the decryption unit 91 of the decryption/encryption module 74 decrypts the content key Kco which was stored in the HDD 52 in step S344 of FIG. 54. In step S370, the encryption unit 93 of the decryption/encryption module 74 encrypts the decrypted content key Kco by use of the temporary key Ktemp. In step S371, the SAM 62 transmits to the extension section 63 the content key Kco having been encrypted by use of the temporary key Ktemp.

[0185] In step S372, the decryption module 76 of the extension section 63 decrypts the content key Kco by use of the temporary key Ktemp. In step S373, the SAM 62 reads the content recorded in the HDD 52 and transmits it to the extension section 63. In step S374, the decryption module 77 of the extension section 63 decrypts the content by use of the content key Kco. In step S375, the extension module 78 of the extension section 63 extends the decrypted content in accordance with a predetermined scheme such as ATRAC2. In step S376, the watermark addition module 79 of the extension section 63 inserts into the extended content a predetermined watermark that specifies the receiver 51. In step S377, the receiver 51 outputs the reproduced content to an unillustrated speaker or the like and then ends the processing.

[0186] When in step S363 the hash value calculated in step S362 is judged not to coincide with the hash value stored in

the storage module 73, in step S378, the SAM 62 performs predetermined error processing, such as processing for causing an unillustrated display unit to display an error message, and then ends the processing.

[0187] In the above-described manner, the receiver 51 reproduces the content.

[0188] FIG. 56 is a flowchart showing processing which the receiver 51 in the user home network 5 having the configuration shown in FIG. 11 performs in order to cause the decoder 56 to reproduce content. Since processing in steps S391 to S397 is the same as that in steps S361 to S367 of FIG. 55, repeated description is omitted here.

[0189] In step S398, the mutual authentication module 71 of the SAM 62 and the mutual authentication module 101 of the decoder 56 mutually authenticate and share the temporary key Ktemp. Since this authentication processing is similar to that having been described with reference to FIGS. 37 to 39, repeated description is omitted here. The random number R1, R2, or R3 used in the mutual authentication is used as a temporary key Ktemp. In step S399, by use of the save key Ksave stored in the storage module 73, the decryption unit 91 of the decryption/encryption module 74 decrypts the content key Kco which was stored in the HDD 52. In step S400, the encryption unit 93 of the decryption/encryption module 74 encrypts the decrypted content key Kco by use of the temporary key Ktemp. In step S401, the SAM 62 transmits to the decoder 56 the content key Kco having been encrypted by

use of the temporary key Ktemp.

[0190] In step S402, the decryption module 102 of the decoder 56 decrypts the content key Kco by use of the temporary key Ktemp. In step S403, the SAM 62 reads the content recorded in the HDD 52 and transmits it to the decoder 56. In step S404, the decryption module 103 of the decoder 56 decrypts the content by use of the content key Kco. In step S405, the extension module 104 of the decoder 56 extends the decrypted content in accordance with a predetermined scheme such as ATRAC2. In step S406, the watermark addition module 105 of the decoder 56 inserts into the extended content a predetermined watermark that specifies the decoder 56. In step S407, the decoder 56 outputs the reproduced content to an unillustrated speaker or the like and then ends the processing.

[0191] Since processing in step S408 is the same as that in step S378 of FIG. 55, repeated description is omitted here.

[0192] As described above, when the user home network 5 has the configuration shown in FIG. 11, the content received by the receiver 51 is reproduced at the decoder 56.

[0193] With reference to the flowchart of FIG. 57, there is described processing which enables the EMD service center 1 to produce a settlement object before performance of settlement processing, which will be described later with reference to FIG. 61. In step S421, the historical-data management section 15 of the EMD service center 1 selects charging information regarding use of specific content, among

a plurality pieces of charging information which the historical-data management section 15 has received from the user home network 5 and stores in, for example, step S187 or S189 of FIG. 47. Subsequently, the historical-data management section 15 transmits the selected charging information to the profit-distribution section 16. In step S422, the profit-distribution section 16 judges whether the charging information received from the historical-data management section 15 contains data showing profit distribution to the content provider 2 and the service provider 3. When the charging information received from the historical-data management section 15 is judged to contain data showing profit distribution to the content provider 2 and the service provider 3, the profit-distribution section 16 proceeds to step S423.

[0194] In step S423, with reference to the data contained in the charging information and indicating profit distribution, the profit-distribution section 16 calculates an amount of money which a user having utilized the specific content must pay to the service provider 3. In step S424, with reference to the data contained in the charging information and indicting profit distribution, the profit-distribution section 16 calculates an amount of money which the service provider 3 must pay to the content provider 2. In step S425, with reference to the data contained in the charging information and indicting profit distribution, the profit-distribution section 16 calculates an amount of money which

the content provider 2 must pay to the proprietary organization. Subsequently the profit-distribution section 16 proceeds to step S429.

[0195] When in step S422 the charging information received from the historical-data management section 15 is judged not to contain data showing profit distribution to the content provider 2 and the service provider 3, the profit-distribution section 16 proceeds to step S426. In step S426, with reference to the profit-distribution database stored in the profit-distribution section 16, the profit-distribution section 16 calculates an amount of money which the user having utilized the specific content must pay to the service provider 3. In step S427, with reference to the profit-distribution database stored in the profit-distribution section 16, the profit-distribution section 16 calculates an amount of money which the service provider 3 must pay to the content provider 2. In step S428, with reference to the profit-distribution database stored in the profit-distribution section 16, the profit-distribution section 16 calculates an amount of money which the content provider 2 must pay to the proprietary organization. Subsequently the profit-distribution section 16 proceeds to step S429.

[0196] In step S429, with reference to data of the discount information database stored in the profit-distribution section 16, the profit-distribution section 16 corrects the amount of money which the specific user must pay to the service provider 3, the amount of money which the service

provider 3 must pay to the content provider 2, and the amount of money which the content provider 2 must pay to the proprietary organization.

[0197] In step S430, the historical-data management section 15 judges whether the calculations in steps S423 to S429 have been performed for all the contents. When it is judged that the calculations in steps S423 to S429 have not yet been performed for all the contents, the historical-data management section 15 returns to step S421 in order to repeat the processing in step 421 and in subsequent steps. When it is judged in step S430 that the calculations in steps S423 to S429 have been performed for all the contents, the profit-distribution section 16 proceeds to step S431.

[0198] In step S431, for each user, the profit-distribution section 16 calculates an amount of money to be paid to each service provider 3 and produces a credit settlement object 1 (e.g., a credit settlement object 1 shown in FIG. 58(A) when the user pays the usage fee by use of a credit card). In the credit settlement object 1, the ID of the user is set as a payer; the ID of the service provider 3 is set as a receiver; and an amount of money to be paid to the service provider 3 is set as a payment amount. In step S432, for each service provider 3, the profit-distribution section 16 calculates an amount of money to be paid to each content provider 2 and produces a credit settlement object 2 (e.g., a credit settlement object 2 shown in FIG. 58(B) when the user pays the usage fee by use of a credit card). In the credit

settlement object 2, the credit settlement object 1 is set as a payer; the ID of the content provider 2 is set as a receiver; and an amount of money to be paid to the content provider 2 is set as a payment amount.

[0199] In step S433, for each content provider 2, the profit-distribution section 16 calculates an amount of money to be paid to the proprietary organization and produces a credit settlement object 3 (e.g., a credit settlement object 3 shown in FIG. 58(C) when the user pays the usage fee by use of a credit card). In the credit settlement object 3, the credit settlement object 1 is set as a payer; the ID of the proprietary organization is set as a receiver; and an amount of money to be paid to the proprietary organization is set as a payment amount. In step S434, with reference to the user's usage-fee table which is stored in the charge billing section 19 and which stores a usage fee that each user pays to the EMD service center 1, the charge billing section 19 calculates an amount of money to be collected from the user and produces a credit settlement object 4 (e.g., a credit settlement object 4 shown in FIG. 58(D) when the user pays the usage fee by use of a credit card). Further, the charge billing section 19 sets the collection money of the credit settlement object 1 and ends the processing. In the credit settlement object 4, the credit settlement object 1 is set as a payer; the ID of the EMD service center 1 is set as a receiver; and an amount of money to be paid to the EMD service center 1 is set as a payment amount.

[0200] In the above-described manner, the EMD service center 1 produces a settlement object.

[0201] FIG. 59 is a diagram showing an example of a bank settlement object used when the service provider 3, the content provider 2, and the proprietary organization pay service charges to the EMD service center 1 by means of bank settlement. In a bank settlement object 1 shown in FIG. 59(A), the ID of the service provider 3 is set as a payer; an amount of money to be collected from the service provider 3 is set as a collection amount; the ID of the EMD service center 1 is set as a receiver; and an amount of money to be paid to the EMD service center 1 (equal to the collection amount) is set as a payment amount. In a bank settlement object 2 shown in FIG. 59(B), the ID of the content provider 2 is set as a payer; an amount of money to be collected from the content provider 2 is set as a collection amount; the ID of the EMD service center 1 is set as a receiver; and an amount of money to be paid to the EMD service center 1 (equal to the collection amount) is set as a payment amount. In a bank settlement object 3 shown in FIG. 59(C), the ID of the proprietary organization is set as a payer; an amount of money to be collected from the proprietary organization is set as a collection amount; the ID of the EMD service center 1 is set as a receiver; and an amount of money to be paid to the EMD service center 1 (equal to the collection amount) is set as a payment amount.

[0202] FIG. 60 is a diagram showing an example of a

settlement object used when each user pays fees by use of a credit card; and the service provider 3 and the content provider 2 perform settlement by use of their bank accounts. Since the credits settlement objects of FIGS. 60(A) and 60(D) are the same as those of FIGS. 58(A) and 58(D), repeated descriptions are omitted. In a bank settlement object 2 shown in FIG. 60(B), the ID of the service provider 3 is set as a payer; an amount of money to be collected from the service provider 3 (the sum of an amount of money to be paid to the content provider 2 and an amount of money to be paid to the proprietary organization) is set as a collection amount; the ID of the content provider 2 is set as a receiver; and an amount of money to be paid to the content provider 2 (equal to the collection amount) is set as a payment amount. In a bank settlement object 3 shown in FIG. 60(C), the ID of the content provider 2 is set as a payer; an amount of money to be collected from the content provider 2 is set as a collection amount; the ID of the proprietary organization is set as a receiver; and an amount of money to be paid to the proprietary organization (equal to the collection amount) is set as a payment amount.

[0203] Upon execution of settlement on the basis of the payers, collection amounts, receivers, and payment amounts described in the settlement objects of FIGS. 58, 59, and 60, predetermined amounts of money are paid to the EMD service center 1, the content provider 2, the service provider 3, and the proprietary organization. Processing which enables the

EMD service center 1 to perform settlement while using a credit settlement object will be described with reference to the flowchart of FIG. 61. In step S451, the treasury section 20 of the EMD service center 1 obtains a settlement institute, such as a bank, which serves as a receiver, from an ID which is described as a receiver in the credit settlement object. In step S452, the treasury section 20 of the EMD service center 1 obtains a settlement institute, such as a credit company, which serves as a payer, from an ID which is described as a payer in the credit settlement object. In step S453, on the basis of previously stored information, the treasury section 20 judges whether credit-check processing must be performed for the payer. When it is judged that credit-check processing for the payer is necessary, in step S454, the treasury section 20 performs the credit-check processing. When the credit-check processing performed in step S454 has revealed that the payer cannot make payment, the treasury section 20 ends the processing. When the credit-check processing performed in step S454 has revealed that the payer can make payment, the treasury section 20 proceeds to step S455.

[0204] When it is judged in step S453 that credit-check processing for the payer is unnecessary, the treasury section 20 skips step S454 and proceeds to step S455.

[0205] In step S455, the treasury section 20 judges whether the processing for the previous settlement object has been completed. When it is judged that the processing for the

previous settlement object has been completed, the treasury section 20 proceeds to step S456 and transmits to the settlement institutes obtained in steps S451 and S452 respective settlement instructions which correspond to the collection amount and payment amount described in the credit settlement object. In step S457, the treasury section 20 transmits the information regarding the settlement processing performed in step S456 to a receiver corresponding to the ID which is described as a receiver in the credit settlement object. In step S458, the treasury section 20 transmits the information regarding the settlement processing performed in step S456 to a payer corresponding to the ID which is described as a payer in the credit settlement object. Subsequently, the treasury section 20 ends the processing.

[0206] When it is judged in step S455 that the processing for the previous settlement object has not been completed, the treasury section 20 proceeds to step S459 and executes predetermined error processing for incomplete settlement; such as processing for transmitting a predetermined message to a payer which is described in the settlement object, processing for which has not been completed.

[0207] In the above-described manner, settlement using credit settlement objects is performed.

[0208] FIG. 62 is a flowchart showing processing which enables the EMD service center 1 to perform settlement while using bank settlement objects. This processing is equivalent to processing which is obtained by removing processing for

credit check (steps S451 and S454) from the settlement processing using credit settlement objects shown in FIG. 61. Since processing in steps S471 and S472 is the same as that in steps S451 and S452 of FIG. 61, repeated description is omitted here. Since processing in steps S473 to S477 is the same as that in steps S455 to S459 of FIG. 61, repeated description is omitted here.

[0209] In the above-described manner, settlement using bank settlement objects is processed together with settlement using credit settlement objects. Thus, predetermined amounts of money are collected from users, the content provider 2, the service provider 3, and the proprietary organization; and predetermined amounts of money are transferred to the EMD service center 1, the content provider 2, the service provider 3, and the proprietary organization.

[0210] The embodiment has been described while music data were used as example content. However, contents are not limited to music data and may be dynamic image data, static image data, document data, or program data. When these data are distributed, a compression scheme suitable for the type of content (e.g., MPEG (Moving Picture Experts Group) for image data) is used. As to watermarks, a watermark suitable for the type of content is used.

[0211] The common key cryptosystem has been described while DES, which is a block cryptosystem, was used as an example. However, FEAL proposed by NTT (Trademark), IDEA (International Data Encryption Algorithm), or stream

cryptosystem in which encryption is performed for each unit consisting of one bit to a few bits may be used.

[0212] In the embodiment, content and a content key Kco are encrypted in common key cryptosystem. However, a public key cryptosystem may be used.

[0213] In the present specification, the term "system" refers to the entire apparatus consisting of a plurality of apparatuses.

[0214] Examples of a provision medium for providing users with a computer program for performing the above-described processing include recording media such as a magnetic disk, a CD-ROM, and solid memories, as well as communication media such as a network and a satellite.

[0215]

[Effect of the Invention] In the information processing apparatus described in claim 1, the information processing method described in claim 6, and the provision medium described in claim 7, data which specify the information, and data which indicate an amount to be paid to each of the information providers for use of the information are stored; the sum total of amounts to be paid to each of the information providers is calculated on the basis of the stored data; and an instruction is issued to a settlement institute to perform settlement for each of the information providers, on the basis of profits gained by each of the information providers. Therefore, settlement processing and profit-calculation processing can be performed more

efficiently.

[Brief Description of the Drawings]

[FIG. 1] Diagram for explaining an EMD system.

[FIG. 2] Block diagram showing the functional configuration of the EMD service center 1.

[FIG. 3] Diagram for explaining transmission of distribution keys Kd by the EMD service center 1.

[FIG. 4] Diagram for explaining transmission of distribution keys Kd by the EMD service center 1.

[FIG. 5] Diagram for explaining transmission of distribution keys Kd by the EMD service center 1.

[FIG. 6] Diagram for explaining transmission of distribution keys Kd by the EMD service center 1.

[FIG. 7] Diagram for explaining the user-registration data base.

[FIG. 8] Block diagram showing the functional configuration of the content provider 2.

[FIG. 9] Block diagram showing the functional configuration of the service provider 3.

[FIG. 10] Block diagram showing the configuration of the user home network 5.

[FIG. 11] Block diagram showing the configuration of the user home network 5.

[FIG. 12] Diagram for describing a content and information accompanying the content.

[FIG. 13] Diagram for explaining a content-provider secure container.

[FIG. 14] Diagram for explaining a certificate of the content provider 2.

[FIG. 15] Diagram for explaining a service-provider secure container.

[FIG. 16] Diagram for explaining a certificate of the service provider 3.

[FIG. 17] Diagram showing a handling policy, price information, and conditions-for-use information.

[FIG. 18] Diagram for explaining single copying and multiple copying.

[FIG. 19] Diagram for explaining a handling policy and price information.

[FIG. 20] Diagram for explaining a handling policy, price information, and conditions-for-use information.

[FIG. 21] Diagram for explaining another configuration of a content and information accompanying the content.

[FIG. 22] Diagram for explaining a service-provider secure container.

[FIG. 23] Diagram showing a configuration of a handling policy, handling control information, price information, and conditions-for-use information.

[FIG. 24] Diagram for explaining another configuration of a content and information accompanying the content.

[FIG. 25] Diagram for explaining a content-provider secure container.

[FIG. 26] Diagram for explaining a service-provider secure container.

[FIG. 27] Diagram for explaining the operation of the EMD service center 1 for collecting data necessary for settlement processing.

[FIG. 28] Diagram showing an example of the profit-distribution data base.

[FIG. 29] Diagram showing an example of the discount table.

[FIG. 30] Diagram showing an example of the user's usage-fee table.

[FIG. 31] Diagram for explaining the operation of the EMD service center 1 when receiving charging information from the user home network 5.

[FIG. 32] Diagram for explaining the operation of the EMD service center 1 for profit distribution processing.

[FIG. 33] Diagram for explaining the operation of the EMD service center 1 for transmitting to the JASRAC information regarding past use of contents.

[FIG. 34] Flowchart for explaining processing for content distribution.

[FIG. 35] Flowchart for explaining processing for content distribution.

[FIG. 36] Flowchart for explaining processing which enables the EMD service center 1 to transmits distribution keys Kd to the content provider 2.

[FIG. 37] Flowchart for explaining the operation of mutual authentication performed between the content provider 2 and the EMD service center 1.

[FIG. 38] Flowchart for explaining the operation of mutual

authentication performed between the content provider 2 and the EMD service center 1.

[FIG. 39] Flowchart for explaining the operation of mutual authentication performed between the content provider 2 and the EMD service center 1.

[FIG. 40] Flowchart for explaining processing which enables registration of the receiver 51 in the EMD service center 1.

[FIG. 41] Diagram for explaining a certificate of the SAM.

[FIG. 42] Diagram for explaining a registration list.

[FIG. 43] Flowchart for explaining processing for transferring data of the SAM 62 to the IC card 55 for backup.

[FIG. 44] Flowchart for explaining processing for transferring data of the SAM 62 to the IC card 55 for backup.

[FIG. 45] Flowchart for explaining processing for causing a new receiver to read backup data from the IC card 55.

[FIG. 46] Flowchart for explaining processing for causing a new receiver to read backup data from the IC card 55.

[FIG. 47] Flowchart for explaining processing which enables the receiver 51 to register the recorder 53 depending thereon in the EMD service center 1.

[FIG. 48] Flowchart for explaining processing which enables the receiver 51 to receive the distribution key Kd from the EMD service center 1.

[FIG. 49] Flowchart for explaining processing which enables the recorder to receive the distribution key Kd.

[FIG. 50] Flowchart for explaining processing which enables the content provider 2 to transmit a content-provider secure

container to the service provider 3.

[FIG. 51] Flowchart for explaining another processing which enables the content provider 2 to transmit a content-provider secure container to the service provider 3.

[FIG. 52] Flowchart for explaining processing which enables the service provider 3 to transmit a service-provider secure container to the receiver 51.

[FIG. 53] Flowchart for explaining processing which enables the service provider 3 to transmit a service-provider secure container to the receiver 51.

[FIG. 54] Flowchart for explaining charging processing of the receiver 51.

[FIG. 55] Flowchart for explaining processing which enables the receiver 51 to reproduce content.

[FIG. 56] Flowchart for explaining processing which enables the receiver 51 to cause the decoder 56 to reproduce the content.

[FIG. 57] Flowchart for explaining settlement-object-production processing of the EMD service center 1.

[FIG. 58] Diagram showing an example of a credit settlement object.

[FIG. 59] Diagram showing an example of a bank settlement object.

[FIG. 60] Diagram showing an example of the credit settlement object and the bank settlement object..

[FIG. 61] Flowchart for explaining credit settlement processing.

[FIG. 62] Flowchart for explaining bank settlement processing.

[Description of Reference Numerals]

1: EMD service center, 2: content provider, 3: service provider, 5: user home network, 15: historical-data management section, 16: profit-distribution section, 18: user management section, 20: treasury section, 42: pricing section, 51: receiver, 56: decoder, 61: communication section, 62: SAM, 63: extension section, 71: mutual authentication module, 72: charge module, 73: storage module, 74: decryption/encryption module, 75: mutual authentication module, 76: decryption module, 77: decryption module, 81: mutual authentication module, 91: decryption unit, 92: encryption unit, 93: encryption unit, 101: mutual authentication module, 102: decryption module, 103: decryption module

FIG. 1

1: EMD SERVICE CENTER

2: CONTENT PROVIDER

3: SERVICE PROVIDER

4: NETWORK

5: USER HOME NETWORK

FIG. 2

11: SERVICE-PROVIDER MANAGEMENT SECTION

12: CONTENT-PROVIDER MANAGEMENT SECTION

13: COPY-RIGHT MANAGEMENT SECTION

14: KEY SERVER

15: HISTORICAL-DATA MANAGEMENT SECTION

16: PROFIT-DISTRIBUTION SECTION

17: MUTUAL AUTHENTICATION SECTION

18: USER MANAGEMENT SECTION

19: CHARGE BILLING SECTION

20: TREASURY SECTION

21: AUDITOR SECTION

A: EMD SERVICE CENTER 1

FIG. 3

A: DISTRIBUTION KEY HELD BY CONTENT PROVIDER

B: DISTRIBUTION KEY HELD BY EMD SERVICE CENTER

C: DISTRIBUTION KEY HELD BY RECEIVER

D: DISTRIBUTION KEYS TO BE USED

E: DISTRIBUTION KEY

F: VERSION OF DISTRIBUTION KEY

G: USABLE PERIOD

H: START

I: END

J: TRANSMISSION OF DISTRIBUTION KEYS

FIG. 4

SAME AS FIG. 3

FIG. 5

SAME AS FIG. 3

FIG. 6

SAME AS FIG. 3

FIG. 7

A: ID

B: SETTLEMENT PROCESSING

C: REGISTRATION

D: CONNECTION WITH EMD SERVICE CENTER

E: POSSIBLE

F: IMPOSSIBLE

FIG. 8

31: CONTENT SERVER

32: WATERMARK ADDING SECTION

33: COMPRESSION SECTION

34: ENCRYPTION SECTION

35: RANDOM-NUMBER GENERATION SECTION

36: ENCRYPTION SECTION

37: POLICY STORAGE SECTION

38: SECURE CONTAINER CREATION SECTION

39: MUTUAL AUTHENTICATION SECTION

A: CONTENT PROVIDER 2

FIG 9

41: CONTENT SERVER

42: PRICING SECTION

43: POLICY STORAGE SECTION

44: SECURE CONTAINER CREATION SECTION

45: MUTUAL AUTHENTICATION SECTION

A: SERVICE PROVIDER 3

FIG. 10

51: RECEIVER

52: HDD

53: RECORDER

54: MD DRIVE

55: IC CARD

61: COMMUNICATION SECTION

62: SAM

63: EXTENSION SECTION

64: IC CARD INTERFACE

65: RECORD/REPRODUCTION SECTION

66: SAM

67: EXTENSION SECTION

71: MUTUAL AUTHENTICATION MODULE

72: CHARGE MODULE

73: STORAGE MODULE

74: DECRYPTION/ENCRYPTION MODULE

75: MUTUAL AUTHENTICATION MODULE

76: DECRYPTION MODULE

77: DECRYPTION MODULE

78: EXTENSION MODULE

79: WATERMARK ADDITION MODULE

80: MUTUAL AUTHENTICATION MODULE

81: STORAGE MODULE

91: DECRYPTION UNIT

92: RANDOM-NUMBER GENERATION UNIT

93: ENCRYPTION UNIT

A: USER HOME NETWORK 5

FIG. 11

56: DECODER

101: MUTUAL AUTHENTICATION MODULE

102: DECRYPTION MODULE

103: DECRYPTION MODULE

104: EXTENSION MODULE

105: WATERMARK ADDITION MODULE

A: USER HOME NETWORK 5

OTHER ELEMENTS ARE THE SAME AS THOSE SHOWN IN FIG. 10

FIG. 12

1: EMD SERVICE CENTER

2: CONTENT PROVIDER

3: SERVICE PROVIDER

5: USER HOME NETWORK

A: CONTENT

B: CONTENT KEY

C: HANDLING POLICY

D: PRICE INFORMATION

E: CONDITIONS-FOR-USE INFORMATION

F: CHARGING INFORMATION

G: ENCRYPTED INFORMATION

H: INFORMATION WITH SIGNATURE

FIG. 13

A: CONTENT-PROVIDER SECURE CONTAINER

B: CONTENT KEY Kco

C: CONTENT

D: DISTRIBUTION KEY Kd

E: HANDLING POLICY

F: PRIVATE KEY Kscp OF CONTENT PROVIDER

G: SIGNATURE

H: HASH FUNCTION

FIG. 14

A: CERTIFICATE OF CONTENT PROVIDER

B: VERSION NUMBER OF CERTIFICATE

C: SERIAL NUMBER OF CERTIFICATE WHICH AUTHENTICATION OFFICE HAS ALLOCATED

D: ALGORITHM AND PARAMETERS USED IN SIGNATURE

E: NAME OF AUTHENTICATION OFFICE

F: VALID TERM OF CERTIFICATE

G: NAME (ID) OF CONTENT PROVIDER

H: PUBLIC KEY Kpcp OF CONTENT PROVIDER

I: PRIVATE KEY Ksca OF AUTHENTICATION OFFICE

J: SIGNATURE

K: HASH FUNCTION

FIG 15

A: SERVICE PROVIDER SECURE CONTAINER

B: CONTENT KEY Kco

C: CONTENT

D: DISTRIBUTION KEY Kd

E: HANDLING POLICY

F: PRICE INFORMATION

G: PRIVATE KEY Kssp OF SERVICE PROVIDER

H: SIGNATURE

I: HASH FUNCTION

FIG. 16

A: CERTIFICATE OF SERVICE PROVIDER

B: VERSION NUMBER OF CERTIFICATE

C: SERIAL NUMBER OF CERTIFICATE WHICH AUTHENTICATION

OFFICE HAS ALLOCATED

D: ALGORITHM AND PARAMETERS USED IN SIGNATURE

E: NAME OF AUTHENTICATION OFFICE

F: VALID TERM OF CERTIFICATE

G: NAME (ID) OF SERVICE PROVIDER

H: PUBLIC KEY Kpsp OF SERVICE PROVIDER

I: PRIVATE KEY Ksca OF AUTHENTICATION OFFICE

J: SIGNATURE

K: HASH FUNCTION

FIG. 17

A: HANDLING POLICY

B: ITEMS OF USE

C: REPRODUCTION

D: SINGLE COPYING

E: MULTICOPYING

F: POSSIBLE/IMPOSSIBLE

G: HANDLING POLICY AND PRICE INFORMATION

H: PRICE

I: 150 YEN

J: 80 YEN

K: CONDITIONS-FOR-USE INFORMATION

FIG. 18

A: MULTICOPYING

B: SINGLE COPYING

C: ORIGINAL

D: COPY

FIG. 19

A: ITEMS OF USE

B: REPRODUCTION

C: SINGLE COPY

D: MULTIPLE COPY

E: HANDLING POLICY AND PROFIT DISTRIBUTION

F: POSSIBLE/IMPOSSIBLE

G: PROFIT DISTRIBUTION

H: HANDLING POLICY, PROFIT DISTRIBUTION, AND PRICE INFORMATION

I: DISTRIBUTION PRICE

J: CHARGING INFORMATION

K: NUMBER OF TIMES OF USE

L: 70 YEN

M: 40 YEN

N: 60 YEN

O: 150 YEN

P: 30 YEN

Q: 80 YEN

FIG. 20

A: HANDLING POLICY AND PRICE INFORMATION

B: ITEMS OF USE

C: REPRODUCTION

D: LIMITLESS

E: LIMITED NUMBER OF TIMES

F: LIMITED PERIOD

G: PRICE

H: 60 YEN

I: 90 YEN

J: CONDITIONS-FOR-USE INFORMATION

FIG. 21

1: EMD SERVICE CENTER

2: CONTENT PROVIDER

3: SERVICE PROVIDER

5: USER HOME NETWORK

A: CONTENT

B: CONTENT KEY

C: HANDLING POLICY

D: PRICE INFORMATION

E: CONDITIONS-FOR-USE INFORMATION

F: CHARGING INFORMATION

H: ENCRYPTED INFORMATION

I: INFORMATION WITH SIGNATURE

G: HANDLING CONTROL INFORMATION

FIG. 22

A: CONTENT-PROVIDER SECURE CONTAINER

B: CONTENT KEY Kco

C: CONTENT

D: DISTRIBUTION KEY Kd

E: HANDLING POLICY

F: HANDLING CONTROL INFORMATION

G: PRICE INFORMATION

H: PRIVATE KEY Kssp OF SERVICE PROVIDER

I: SIGNATURE

J: HASH FUNCTION

FIG. 23

A: ITEMS OF USE

B: REPRODUCTION

C: SINGLE COPYING

D: MULTICOPYING

E: POSSIBLE/IMPOSSIBLE

F: PRICE

G: CONDITIONS-FOR-USE INFORMATION

H: 150 YEN

I: 80 YEN

J: HANDLING POLICY

K: HANDLING CONTROL INFORMATION AND PRICE INFORMATION

FIG. 24

1: EMD SERVICE CENTER

2: CONTENT PROVIDER

3: SERVICE PROVIDER

5: USER HOME NETWORK

A: CONTENT

B: CONTENT KEY

C: HANDLING POLICY

D: PRICE INFORMATION

E: CONDITIONS-FOR-USE INFORMATION

F: CHARGING INFORMATION

G: HANDLING CONTROL INFORMATION

H: ENCRYPTED INFORMATION

FIG. 25

A: CONTENT-PROVIDER SECURE CONTAINER

B: CONTENT KEY Kco

C: CONTENT

D: DISTRIBUTION KEY Kd

E: HANDLING POLICY

F: PRIVATE KEY Kscp OF CONTENT PROVIDER

G: SIGNATURE

H: HASH FUNCTION

FIG. 26

A: SERVICE-PROVIDER SECURE CONTAINER

B: CONTENT KEY Kco

C: CONTENT

D: DISTRIBUTION KEY Kd

E: HANDLING POLICY

F: HANDLING CONTROL INFORMATION

G: PRICE INFORMATION

H: PRIVATE KEY Kssp OF SERVICE PROVIDER

I: SIGNATURE

J: HASH FUNCTION

FIG. 27

1: EMD SERVICE CENTER

2: CONTENT PROVIDER

3: SERVICE PROVIDER

5: USER HOME NETWORK

A: CONTENT-PROVIDER REGISTRATION DATA

B:: CONTENT-PROVIDER ID

C: SERVICE-PROVIDER REGISTRATION DATA

D: SERVICE-PROVIDER ID

E: USER ID

F: USER-REGISTRATION DATA

FIG. 28

A: CONTENT ID

B: CONTENT-PROVIDER ID

C: PROPRIETOR ORGANIZATION

FIG. 29

A: PROVIDER ID

B: CONTENT PROVIDER 1

C: CONTENT PROVIDER 2

D: SERVICE PROVIDER 1

E: SERVICE PROVIDER 2

F: CONTENT ID

G: DISCOUNT RATE

H: PERIOD

I: ALL CONTENTS

FIG. 30

A: MONTHLY BASIC CHARGE

B: 1000 YEN

C: PERIOD

D: USAGE FEE

E: ADJUSTMENT AMOUNT

F: ABOVE 3000 YEN

FIG. 31

1: EMD SERVICE CENTER

2: CONTENT PROVIDER

3: SERVICE PROVIDER

5: USER HOME NETWORK

11: SERVICE-PROVIDER MANAGEMENT SECTION

12: CONTENT-PROVIDER MANAGEMENT SECTION

13: COPY-RIGHT MANAGEMENT SECTION

14: KEY SERVER

15: HISTORICAL-DATA MANAGEMENT SECTION

16: PROFIT-DISTRIBUTION SECTION

17: MUTUAL AUTHENTICATION SECTION

18: USER MANAGEMENT SECTION

19: CHARGE BILLING SECTION

20: TREASURY SECTION

21: AUDITOR SECTION

FIG. 32

SAME AS FIG. 31

FIG. 33

SAME AS FIG. 31

FIG. 34

A: START CONTENT DISTRIBUTION PROCESSING

S11: EMD SERVICE CENTER TRANSMITS DISTRIBUTION KEYS TO CONTENT PROVIDER, AND CONTENT PROVIDER RECEIVES DISTRIBUTION KEYS

S12: USER REGISTERS APPARATUS INFORMATION IN EMD SERVICE CENTER

S13: EMD SERVICE CENTER TRANSMITS DISTRIBUTION KEYS TO USER, AND USER RECEIVES DISTRIBUTION KEYS

S14: CONTENT PROVIDER TRANSMITS SECURE CONTAINER TO SERVICE PROVIDER, AND SERVICE PROVIDER RECEIVES SECURE CONTAINER

S15: SERVICE PROVIDER TRANSMITS SECURE CONTAINER TO USER, AND USER RECEIVES SECURE CONTAINER

S16: USER PERFORMS CHARGING PROCESSING

S17: USER REPRODUCES CONTENT

B: END

FIG. 35

A: START CONTENT DISTRIBUTION PROCESSING

S21: EMD SERVICE CENTER TRANSMITS DISTRIBUTION KEYS TO CONTENT PROVIDER, AND CONTENT PROVIDER RECEIVES DISTRIBUTION KEYS

S22: EMD SERVICE CENTER TRANSMITS DISTRIBUTION KEYS TO SERVICE PROVIDER, AND SERVICE PROVIDER RECEIVES DISTRIBUTION KEYS

S23: USER REGISTERS APPARATUS INFORMATION IN EMD SERVICE CENTER

S24: EMD SERVICE CENTER TRANSMITS DISTRIBUTION KEYS TO USER, AND USER RECEIVES DISTRIBUTION KEYS

S25: CONTENT PROVIDER TRANSMITS SECURE CONTAINER TO SERVICE PROVIDER, AND SERVICE PROVIDER RECEIVES SECURE CONTAINER

S26: SERVICE PROVIDER TRANSMITS SECURE CONTAINER TO USER, AND USER RECEIVES SECURE CONTAINER

S27: USER PERFORMS CHARGING PROCESSING

S28: USER REPRODUCES CONTENT

B: END

FIG. 36

A: START PROCESSING FOR TRANSMITTING DISTRIBUTION KEYS TO CONTENT PROVIDER

S31: MUTUAL AUTHENTICATION WITH CONTENT PROVIDER

S32: CONTENT PROVIDER RECEIVES DISTRIBUTION KEYS

S33: CONTENT PROVIDER STORES DISTRIBUTION KEYS

B: RETURN

FIG. 37

1: EMD SERVICE CENTER

2: CONTENT PROVIDER

S41: GENERATE RANDOM NUMBER R1 OF 64 BITS

S42: ENCRYPT R1 BY USE OF KEY Kc

S43: TRANSMIT ENCRYPTED R1 TO EMD SERVICE CENTER

S44: DECRYPT RECEIVED R1

S45: GENERATE RANDOM NUMBER R2 OF 32 BITS

S46: REPLACE LOWER 32 BITS OF RANDOM NUMBER R1 WITH RANDOM NUMBER R2 TO THEREBY OBTAIN $R1_H||R2$

S47: ENCRYPT $R1_H||R2$ BY USE OF KEY Kc

S48: TRANSMIT ENCRYPTED $R1_H||R2$ TO CONTENT PROVIDER

S49: DECRYPT RECEIVED $R1_H||R2$

S50: AUTHENTICATE EMD SERVICE CENTER WHEN UPPER 32 BITS OF DECRYPTED $R1_H||R2$ COINCIDE

S51: GENERATE RANDOM NUMBER R3 OF 32 BITS

S52: FORM R2||R3

S53: ENCRYPT R2||R3 BY USE OF KEY Kc

S54: TRANSMIT ENCRYPTED R2||R3 TO EMD SERVICE CENTER

S55: DECRYPT RECEIVED R2||R3

S56: AUTHENTICATE CONTENT PROVIDER WHEN UPPER 32 BITS OF R2||R3 COINCIDE

FIG. 38

1: EMD SERVICE CENTER

2: CONTENT PROVIDER

S61: GENERATE RANDOM NUMBER R1 OF 64 BITS

S62: ENCRYPT R1 BY USE OF KEY Kc1

S63: TRANSMIT ENCRYPTED R1 TO EMD SERVICE CENTER

S64: DECRYPT RECEIVED R1

S65: ENCRYPT R1 BY USE OF KEY Kc2

S66: GENERATE RANDOM NUMBER R2 OF 64 BITS

S67: ENCRYPT R2 BY USE OF KEY Kc2

S68: TRANSMIT ENCRYPTED R1 AND R2 TO CONTENT PROVIDER

S69: DECRYPT RECEIVED R1 AND R2

S70: AUTHENTICATE EMD SERVICE CENTER WHEN DECRYPTED R1 COINCIDE

S71: ENCRYPT R2 BY USE OF KEY Kc1

S72: TRANSMIT ENCRYPTED R2 TO EMD SERVICE CENTER

S73: DECRYPT RECEIVED R2

S74: AUTHENTICATE CONTENT PROVIDER WHEN DECRYPTED R2 COINCIDE

FIG. 39

1: EMD SERVICE CENTER

2: CONTENT PROVIDER

S81: GENERATE RANDOM NUMBER R1 OF 64 BITS

S82: TRANSMIT R1 AND CERTIFICATE TO EMD SERVICE CENTER

S83: CHECK SIGNATURE OF CERTIFICATE AND WHEN PROPER, EXTRACT PUBLIC KEY Kpcp FROM CERTIFICATE

S84: GENERATE RANDOM NUMBER R2 OF 64 BITS

S85: FORM R1||R2

S86: ENCRYPT R1||R2 BY USE OF PRIVATE KEY Ksesc

S87: ENCRYPT R1||R2 BY USE OF PUBLIC KEY Kpcp

S88: TRANSMIT TO CONTENT PROVIDER R1||R2 ENCRYPTED BY USE OF PRIVATE KEY Ksesc, R1||R2 ENCRYPTED BY USE OF PUBLIC KEY Kpcp,

AND CERTIFICATE

S89: CHECK SIGNATURE OF CERTIFICATE AND WHEN PROPER, EXTRACT PUBLIC KEY Kpesc FROM CERTIFICATE

S90: DECRYPT R1||R2 BY USE OF PUBLIC KEY Kpesc

S91: DECRYPT R1||R2 BY USE OF PRIVATE KEY Kscp

S92: AUTHENTICATE EMD SERVICE CENTER WHEN DECRYPTED R1||R2 COINCIDE

S93: GENERATE RANDOM NUMBER R3 OF 64 BITS

S94: FORM R2||R3

S95: ENCRYPT R2||R3 BY USE OF PUBLIC KEY Kpesc

S96: TRANSMIT ENCRYPTED R2||R3 TO EMD SERVICE CENTER

S97: DECRYPT R2||R3 BY USE OF PRIVATE KEY Ksesc

S98: AUTHENTICATE CONTENT PROVIDER WHEN DECRYPTED R2 COINCIDE

FIG. 40

A: START REGISTRATION PROCESSING

S101: IS IC CARD FOR BACKUP ATTACHED?

S102: PROCESSING FOR READING BACKUP

S103: SAM MUTUALLY AUTHENTICATES WITH EMD SERVICE CENTER AND TRANSMITS CERTIFICATE

S104: SAM ENCRYPTS INFORMATION OF SETTLEMENT INSTITUTE OF USER, ETC. BY USE OF TEMPORARY KEY AND TRANSMITS THEM TO EMD SERVICE CENTER

S105: EMD SERVICE CENTER SEARCHES REGISTRATION DATA BASE BY USE OF ID OF SAM

S106: IS SAM OF RECEIVED ID REGISTERABLE?

S107: IS SAM OF RECEIVED ID NEW REGISTRATION?

S108: EMD SERVICE CENTER PRODUCES REGISTRATION LIST OF UPDATE REGISTRATION

S109: EMD SERVICE CENTER TRANSFERS TO SAM DISTRIBUTION KEY ENCRYPTED BY USE OF TEMPORARY KEY

S110: SAME DECRYPTS AND STORES RECEIVED DISTRIBUTION KEY

S111: EMD SERVICE CENTER TRANSMITS TO SAM REGISTRATION LIST ENCRYPTED BY USE OF TEMPORARY KEY

S112: SAM DECRYPTS AND STORES RECEIVED REGISTRATION LIST

S113: EMD SERVICE CENTER PRODUCES REGISTRATION LIST OF REGISTRATION DENIAL

S114: EMD SERVICE CENTER PRODUCES NEW REGISTRATION LIST

B: RETURN

FIG. 41

A: CERTIFICATE OF SAM

B: VERSION NUMBER OF CERTIFICATE

C: SERIAL NUMBER OF CERTIFICATE WHICH AUTHENTICATION OFFICE HAS ALLOCATED

D: ALGORITHM AND PARAMETERS USED IN SIGNATURE

E: NAME OF AUTHENTICATION OFFICE

F: VALID TERM OF CERTIFICATE

G: NAME (ID) OF SAM

H: PUBLIC KEY Kpu OF SAM

I: PARAMETER INDICATING WHERE TO DEPEND ON ANOTHER SAM

J: PRIVATE KEY Ksca OF AUTHENTICATION OFFICE

K: SIGNATURE

L: HASH FUNCTION

FIG. 42

A: ID OF SAM

B: REGISTRATION DENIAL FLAG

C: STATUS FLAG

D: CONDITION FLAG

E: SIGNATURE

FIG. 43

A: START BACKUP OF STORAGE DATA OF SAM

S121: SAM MUTUALLY AUTHENTICATES WITH IC CARD

S122: GENERATE RANDOM NUMBER AS BACKUP KEY

S123: ENCRYPT STORAGE DATA OF SAM BY USE OF BACKUP KEY

S124: ENCRYPT BACKUP KEY BY USE OF PUBLIC KEY OF EMD SERVICE CENTER

S125: STORE ENCRYPTED STORAGE DATA OF SAM AND ENCRYPTED BACKUP KEY IN IC CARD

B: END

FIG. 44

A: START BACKUP OF STORAGE DATA OF SAM

S131: SAM MUTUALLY AUTHENTICATES WITH IC CARD

S132: ENCRYPT STORAGE DATA OF SAM BY USE OF PUBLIC KEY OF EMD SERVICE CENTER

S133: STORE ENCRYPTED STORAGE DATA OF SAM IN IC CARD

B: END

FIG. 45

A: START PROCESSING FOR READING BACKUP INTO NEW RECEIVER

S141: SAM MUTUALLY AUTHENTICATES WITH IC CARD

S142: READ ENCRYPTED STORAGE DATA OF SAM AND ENCRYPTED BACKUP KEY FROM IC CARD

S143 SAM MUTUALLY AUTHENTICATES WITH EMD SERVICE CENTER

S144: SAM TRANSMITS ENCRYPTED STORAGE DATA OF SAM AND ENCRYPTED BACKUP KEY TO EMD SERVICE CENTER

S145: EMD SERVICE CENTER DECRYPTS BACKUP KEY BY USE OF PRIVATE KEY

S146: EMD SERVICE CENTER DECRYPTS STORAGE DATA OF SAM BY USE OF BACKUP KEY

S147: EMD SERVICE CENTER ENCRYPTS STORAGE DATA OF SAM BY USE OF TEMPORARY KEY

S148: EMD SERVICE CENTER TRANSMITS STORAGE DATA OF SAM

S149: SAM DECRYPTS AND STORES RECEIVED DATA

S150: EMD SERVICE CENTER MAKES ID OF OLD SAM UN-REGISTERABLE RETURN

FIG. 46

A: START PROCESSING FOR READING BACKUP INTO NEW RECEIVER

S161: SAM MUTUALLY AUTHENTICATES WITH IC CARD

S162: READ ENCRYPTED STORAGE DATA OF SAM FROM IC CARD

S163 SAM MUTUALLY AUTHENTICATES WITH EMD SERVICE CENTER

S164: SAM TRANSMITS ENCRYPTED STORAGE DATA OF SAM TO EMD SERVICE CENTER

S165: EMD SERVICE CENTER DECRYPTS STORAGE DATA OF SAM BY USE

OF PRIVATE KEY

S166: EMD SERVICE CENTER ENCRYPTS STORAGE DATA OF SAM BY USE OF TEMPORARY KEY

S167: EMD SERVICE CENTER TRANSMITS STORAGE DATA OF SAM

S168: SAM DECRYPTS AND STORES RECEIVED DATA

S169: EMD SERVICE CENTER MAKES ID OF OLD SAM UN-REGISTERABLE RETURN

FIG. 47

A: START PROCESSING FOR REGISTERING RECORDER

S181: RECEIVER ADDS ID OF RECORDER INTO REGISTRATION LIST

S182: RECEIVER AND EMD SERVICE CENTER PERFORM MUTUAL AUTHENTICATION

S183: IS RECEIVER UN-REGISTERABLE?

S184: RECEIVER TRANSMITS TO EMD SERVICE CENTER VERSION OF DISTRIBUTION KEY OF RECEIVER, CHARGING INFORMATION, HANDLING POLICY, AND REGISTRATION LIST, WHICH HAVE BEEN ENCRYPTED BY USE OF TEMPORARY KEY

S185: EMD SERVICE CENTER DECRYPTS RECEIVED DATA, PROCESSES CHARGING INFORMATION, AND UPDATES REGISTRATION LIST

S186: IS DISTRIBUTION KEY OF RECEIVER NEWEST VERSION?

S187: EMD SERVICE CENTER TRANSMITS REGISTRATION LIST AND CHARGING-INFORMATION RECEIPT MESSAGE ENCRYPTED BY USE OF TEMPORARY KEY, AND RECEIVER RECEIVES AND STORES REGISTRATION LIST AND CHARGING-INFORMATION RECEIPT MESSAGE

S188: RECEIVER ERASES CHARGING INFORMATION AND UPDATES REGISTRATION LIST

S189: EMD SERVICE CENTER TRANSMITS REGISTRATION LIST, CHARGING-INFORMATION RECEIPT MESSAGE, AND DISTRIBUTION KEY ENCRYPTED BY USE OF TEMPORARY KEY, AND RECEIVER RECEIVES AND STORES REGISTRATION LIST, CHARGING-INFORMATION RECEIPT MESSAGE, AND DISTRIBUTION KEY

S190: RECEIVER ERASES CHARGING INFORMATION AND UPDATES REGISTRATION LIST AND DISTRIBUTION KEY

S191: IS RECORDER UN-REGISTERABLE?

S192: RECEIVER AND RECORDER PERFORM MUTUAL AUTHENTICATION

S193: RECEIVER TRANSMITS REGISTRATION COMPLETION MESSAGE AND DISTRIBUTION KEY ENCRYPTED BY USE OF TEMPORARY KEY, AND RECORDER RECEIVES AND DECRYPTS REGISTRATION COMPLETION MESSAGE AND DISTRIBUTION KEY

S194: RECORDER UPDATES DISTRIBUTION KEY

B: RETURN

FIG. 48

A: START PROCESSING OF RECEIVER FOR RECEIVING DISTRIBUTION KEY

S201: RECEIVER MUTUALLY AUTHENTICATES WITH EMD SERVICE CENTER

S202: RECEIVER TRANSMITS CERTIFICATE TO EMD SERVICE CENTER

S203: IS RECEIVER UN-REGISTERABLE?

S204: RECEIVER TRANSMITS TO EMD SERVICE CENTER VERSION OF DISTRIBUTION KEY, CHARGING INFORMATION, HANDLING POLICY, AND REGISTRATION LIST, WHICH HAVE BEEN ENCRYPTED BY USE OF TEMPORARY KEY

S205: EMD SERVICE CENTER DECRYPTS RECEIVED DATA, AND

PROCESSES CHARGING INFORMATION

S206: IS DISTRIBUTION KEY NEWEST VERSION?

S207: EMD SERVICE CENTER TRANSMITS REGISTRATION LIST AND CHARGING-INFORMATION RECEIPT MESSAGE ENCRYPTED BY USE OF TEMPORARY KEY, AND RECEIVER RECEIVES AND DECRYPTS REGISTRATION LIST AND CHARGING-INFORMATION RECEIPT MESSAGE

S208: RECEIVER ERASES CHARGING INFORMATION AND UPDATES REGISTRATION LIST

S209: EMD SERVICE CENTER TRANSMITS REGISTRATION LIST, CHARGING-INFORMATION RECEIPT MESSAGE, AND DISTRIBUTION KEY ENCRYPTED BY USE OF TEMPORARY KEY, AND RECEIVER RECEIVES AND DECRYPTS REGISTRATION LIST, CHARGING-INFORMATION RECEIPT MESSAGE, AND DISTRIBUTION KEY

S210: RECEIVER ERASES CHARGING INFORMATION AND UPDATES REGISTRATION LIST AND DISTRIBUTION KEY

B: RETURN

FIG. 49

A: START PROCESSING OF RECORDER FOR RECEIVING DISTRIBUTION KEY

S221: RECEIVER AND RECORDER PERFORM MUTUAL AUTHENTICATION

S222: IS RECORDER INCLUDED IN REGISTRATION LIST OF RECEIVER

S223: IS RECORDER UN-REGISTERABLE?

S224: RECORDER TRANSMITS TO RECEIVER VERSION OF DISTRIBUTION KEY AND CHARGING INFORMATION WHICH HAVE BEEN ENCRYPTED BY USE OF TEMPORARY KEY, AND RECEIVER RECEIVES AND DECRYPTS VERSION OF DISTRIBUTION KEY AND CHARGING INFORMATION

S225: RECEIVER AND EMD SERVICE CENTER PERFORM MUTUAL AUTHENTICATION

S226: IS RECEIVER UN-REGISTERABLE?

S227: RECEIVER TRANSMITS TO EMD SERVICE CENTER VERSION OF DISTRIBUTION KEY, CHARGING INFORMATION, HANDLING POLICY, AND REGISTRATION LIST OF RECEIVER, AS WELL AS CHARGING INFORMATION OF RECORDER, WHICH HAVE BEEN ENCRYPTED BY USE OF TEMPORARY KEY

S228: EMD SERVICE CENTER DECRYPTS RECEIVED DATA, AND PROCESSES CHARGING INFORMATION

S229: IS DISTRIBUTION KEY OF RECEIVER NEWEST VERSION?

S230: EMD SERVICE CENTER TRANSMITS REGISTRATION LIST AND CHARGING-INFORMATION RECEIPT MESSAGE ENCRYPTED BY USE OF TEMPORARY KEY, AND RECEIVER RECEIVES AND DECRYPTS REGISTRATION LIST AND CHARGING-INFORMATION RECEIPT MESSAGE

S231: RECEIVER ERASES CHARGING INFORMATION AND UPDATES REGISTRATION LIST

S232: EMD SERVICE CENTER TRANSMITS REGISTRATION LIST, CHARGING-INFORMATION RECEIPT MESSAGE, AND DISTRIBUTION KEY ENCRYPTED BY USE OF TEMPORARY KEY, AND RECEIVER RECEIVES AND DECRYPTS REGISTRATION LIST, CHARGING-INFORMATION RECEIPT MESSAGE, AND DISTRIBUTION KEY

S233: RECEIVER ERASES CHARGING INFORMATION AND UPDATES REGISTRATION LIST AND DISTRIBUTION KEY

S234: IS RECORDER UN-REGISTERABLE?

S235: RECEIVER TRANSMITS CHARGING-INFORMATION RECEIPT MESSAGE AND DISTRIBUTION KEY ENCRYPTED BY USE OF TEMPORARY KEY, AND

RECORDER RECEIVES AND DECRYPTS CHARGING-INFORMATION RECEIPT MESSAGE AND DISTRIBUTION KEY

S236: RECORDER ERASES CHARGING INFORMATION AND UPDATES DISTRIBUTION KEY

S237: REGISTER RECORDER

B: RETURN

FIG. 50

A: START PROCESSING FOR TRANSMITTING SECURE CONTAINER TO SERVICE PROVIDER

S251: INSERT WATERMARK INTO CONTENT

S252: COMPRESS CONTENT

S253: GENERATE RANDOM NUMBER AS CONTENT KEY

S254: ENCRYPT CONTENT BY USE OF CONTENT KEY

S255: ENCRYPT CONTENT KEY BY USE OF DISTRIBUTION KEY

S256: CREATE SIGNATURE

S257: CREATE SECURE CONTAINER

S258: MUTUALLY AUTHENTICATE WITH SERVICE PROVIDER

S259: TRANSMIT SECURE CONTAINER

B: RETURN

FIG. 51

A: START PROCESSING FOR TRANSMITTING SECURE CONTAINER TO SERVICE PROVIDER

S271: INSERT WATERMARK INTO CONTENT

S272: COMPRESS CONTENT

S273: GENERATE RANDOM NUMBER AS CONTENT KEY

S274: ENCRYPT CONTENT BY USE OF CONTENT KEY

S275: ENCRYPT CONTENT KEY AND HANDLING POLICY BY USE OF DISTRIBUTION KEY

S276: CREATE SIGNATURE

S277: CREATE SECURE CONTAINER

S278: MUTUALLY AUTHENTICATE WITH SERVICE PROVIDER

S279: TRANSMIT SECURE CONTAINER

B: RETURN

FIG. 52

A: START PROCESSING FOR TRANSMITTING SECURE CONTAINER TO RECEIVER

S291: EXTRACT PUBLIC KEY FROM CERTIFICATE OF SECURE CONTAINER

S292: CONFIRM THAT SECURE CONTAINER HAS NOT BEEN TAMPERED

S293: EXTRACT HANDLING POLICY FROM SECURE CONTAINER

S294: PRODUCE PRICE INFORMATION

S295: CREATE SECURE CONTAINER

S296: MUTUALLY AUTHENTICATE WITH RECEIVER

S299: TRANSMIT SECURE CONTAINER

B: RETURN

FIG. 53

A: START PROCESSING FOR TRANSMITTING SECURE CONTAINER TO RECEIVER

S311: EXTRACT PUBLIC KEY FROM CERTIFICATE OF SECURE CONTAINER

S312: CONFIRM THAT SECURE CONTAINER HAS NOT BEEN TAMPERED

S313: DECRYPTS HANDLING POLICY OF SECURE CONTAINER BY USE OF DISTRIBUTION KEY

S314: PRODUCE HANDLING CONTROL INFORMATION

S315: PRODUCE PRICE INFORMATION

S316: CREATE SECURE CONTAINER

S317: MUTUALLY AUTHENTICATE WITH RECEIVER

S318: TRANSMIT SECURE CONTAINER

B: RETURN

FIG. 54

A: START CHARGING PROCESSING

S331: CAN CONTENT KEY BE DECRYPTED BY USE OF DISTRIBUTION KEY?

S332: PROCESSING FOR RECEIVING DISTRIBUTION KEY

S333: DECRYPTS CONTENT KEY BY USE OF DISTRIBUTION KEY?

S334: PRODUCE CHARGING INFORMATION AND CONDITIONS-FOR-USE FROM HANDLING POLICY AND PRICE INFORMATION

S335: IS TOTAL OF CHARGES UPPER LIMIT?

S336: PROCESSING FOR RECEIVING DISTRIBUTION KEY

S337: STORE CHARGING INFORMATION IN SAM

S338: RECORD CONDITIONS-FOR-USE INFORMATION IN HDD

S339: RECORD HANDLING POLICY IN HDD

S340: CALCULATE HASH VALUE OF CONDITIONS-FOR-USE INFORMATION

S341: STORE HASH VALUE OF CONDITIONS-FOR-USE INFORMATION IN SAM

S342: GENERATE RANDOM NUMBER AS SAVE KEY

S343: ENCRYPT CONTENT KEY BY USE OF SAVE KEY

S344: RECORD CONTENT KEY IN HDD

S345: STORE SAVE KEY IN SAM

B: RETURN

FIG. 55

A: START REPRODUCTION PROCESSING

S361: READ CONDITIONS-FOR-USE INFORMATION AND CONTENT KEY FROM HDD

S362: CALCULATE HASH VALUE OF CONDITIONS-FOR-USE INFORMATION

S363: COINCIDE WITH HASH VALUE WITHIN SAM?

S364: UPDATE CONDITIONS-FOR-USE INFORMATION

S365: CALCULATE HASH VALUE OF CONDITIONS-FOR-USE INFORMATION

S366: STORE HASH VALUE IN SAM

S367: STORE CONDITIONS-FOR-USE INFORMATION IN HDD

S368: SAM AND EXTENSION SECTION PERFORM MUTUAL AUTHENTICATION AND SHARE TEMPORARY KEY

S369: DECRYPT CONTENT KEY BY USE OF SAVE KEY

S370: ENCRYPT CONTENT KEY BY USE OF TEMPORARY KEY

S371: TRANSMIT CONTENT KEY TO EXTENSION SECTION

S372: DECRYPT CONTENT KEY BY USE OF TEMPORARY KEY

S373: TRANSMIT CONTENT TO EXTENSION SECTION

S374: DECRYPT CONTENT BY USE OF CONTENT KEY

S375: EXTEND CONTENT

S376: ADD WATERMARK TO CONTENT

S377: OUTPUT CONTENT

S378: ERROR PROCESSING

B: RETURN

FIG. 56

A: START REPRODUCTION PROCESSING

S391: READ CONDITIONS-FOR-USE INFORMATION AND CONTENT KEY FROM HDD

S392: CALCULATE HASH VALUE OF CONDITIONS-FOR-USE INFORMATION

S393: COINCIDE WITH HASH VALUE WITHIN SAM?

S394: UPDATE CONDITIONS-FOR-USE INFORMATION

S395: CALCULATE HASH VALUE OF CONDITIONS-FOR-USE INFORMATION

S396: STORE HASH VALUE IN SAM

S397: STORE CONDITIONS-FOR-USE INFORMATION IN HDD

S398: SAM AND DECODER PERFORM MUTUAL AUTHENTICATION AND SHARE TEMPORARY KEY

S399: DECRYPT CONTENT KEY BY USE OF SAVE KEY

S400: ENCRYPT CONTENT KEY BY USE OF TEMPORARY KEY

S401: TRANSMIT CONTENT KEY TO DECODER

S402: DECRYPT CONTENT KEY BY USE OF TEMPORARY KEY

S403: TRANSMIT CONTENT TO DECODER

S404: DECRYPT CONTENT BY USE OF CONTENT KEY

S405: EXTEND CONTENT

S406: ADD WATERMARK TO CONTENT

S407: OUTPUT CONTENT

S408: ERROR PROCESSING

B: RETURN

FIG. 57

A: START PROCESSING FOR PRODUCING SETTLEMENT OBJECTS

S421: SELECT CHARGING INFORMATION REGARDING USE OF CERTAIN CONTENT

S422: DOES CHARGING INFORMATION INCLUDE PROFIT DISTRIBUTION TO CONTENT PROVIDER AND SERVICE PROVIDER?

S423: CALCULATE AMOUNT WHICH USER MUST PAY TO SERVICE PROVIDER WITH REFERENCE TO PROFIT DISTRIBUTION OF CHARGING INFORMATION

S424: CALCULATE AMOUNT WHICH SERVICE PROVIDER MUST PAY TO CONTENT PROVIDER WITH REFERENCE TO PROFIT DISTRIBUTION OF CHARGING INFORMATION

S425: CALCULATE AMOUNT WHICH CONTENT PROVIDER MUST PAY TO PROPRIETARY ORGANIZATION WITH REFERENCE TO PROFIT DISTRIBUTION OF CHARGING INFORMATION

S426: CALCULATE AMOUNT WHICH USER MUST PAY TO SERVICE PROVIDER WITH REFERENCE TO PROFIT-DISTRIBUTION DATA BASE

S427: CALCULATE AMOUNT WHICH SERVICE PROVIDER MUST PAY TO CONTENT PROVIDER WITH REFERENCE TO PROFIT-DISTRIBUTION DATA BASE

S428: CALCULATE AMOUNT WHICH CONTENT PROVIDER MUST PAY TO PROPRIETARY ORGANIZATION WITH REFERENCE TO PROFIT-DISTRIBUTION DATA BASE

S429: CORRECT INDIVIDUAL PAYMENT AMOUNTS WITH REFERENCE TO DISCOUNT INFORMATION DATA BASE

S430: HAS CALCULATION BEEN PERFORMED FOR ALL CONTENTS?

S431: CALCULATE AMOUNT WHICH USER MUST PAY TO EACH SERVICE PROVIDER AND PRODUCE SETTLEMENT OBJECT 1

S432: CALCULATE AMOUNT WHICH EACH SERVICE PROVIDER MUST PAY

TO EACH CONTENT PROVIDER AND PRODUCE SETTLEMENT OBJECT 2

S433: CALCULATE AMOUNT WHICH EACH CONTENT PROVIDER MUST PAY TO PROPRIETARY ORGANIZATION AND PRODUCE SETTLEMENT OBJECT 3

S434: DETERMINE AMOUNT TO BE COLLECTED FROM USER, WITH REFERENCE TO SERVICE CHARGE OF EMD SERVICE CENTER AND PRODUCE SETTLEMENT OBJECT 4

B: END

FIG. 58

A:

CREDIT SETTLEMENT

OBJECT 1

PAYER: ID OF USER

COLLECTION AMOUNT: x

RECEIVER: ID OF SERVICE PROVIDER

PAYMENT AMOUNT: x1

B:

CREDIT SETTLEMENT

OBJECT 2

PAYER: CREDIT SETTLEMENT OBJECT 1

COLLECTION AMOUNT: -

RECEIVER: ID OF CONTENT PROVIDER

PAYMENT AMOUNT: x2

C :

CREDIT SETTLEMENT

OBJECT 3

PAYER: CREDIT SETTLEMENT OBJECT 1

COLLECTION AMOUNT: -

RECEIVER: ID OF PROPRIETARY ORGANIZATION

PAYMENT AMOUNT: x3

D :

CREDIT SETTLEMENT

OBJECT 4

PAYER: CREDIT SETTLEMENT OBJECT 1

COLLECTION AMOUNT: -

RECEIVER: ID OF EMD SERVICE CENTER

PAYMENT AMOUNT: x4

FIG. 59

A:

BANK SETTLEMENT

OBJECT 1

PAYER: ID OF SERVICE PROVIDER

COLLECTION AMOUNT: y1

RECEIVER: ID OF EMD SERVICE CENTER

PAYMENT AMOUNT: y1

B:

BANK SETTLEMENT

OBJECT 2

PAYER: ID OF CONTENT PROVIDER

COLLECTION AMOUNT: y2

RECEIVER: ID OF EMD SERVICE CENTER

PAYMENT AMOUNT: y2

C:

BANK SETTLEMENT

OBJECT 3

PAYER: ID OF PROPRIETARY ORGANIZATION

COLLECTION AMOUNT: y3

RECEIVER: ID OF EMD SERVICE CENTER

PAYMENT AMOUNT: y3

FIG. 60

A:

CREDIT SETTLEMENT

OBJECT 1

PAYER: ID OF USER

COLLECTION AMOUNT: x

RECEIVER: ID OF SERVICE PROVIDER

PAYMENT AMOUNT: x1

B:

BANK SETTLEMENT

OBJECT 2

PAYER: ID OF SERVICE PROVIDER

COLLECTION AMOUNT: x2 + x3

RECEIVER: ID OF CONTENT PROVIDER

PAYMENT AMOUNT: x2 + x3

C:

BANK SETTLEMENT

OBJECT 3

PAYER: ID OF CONTENT PROVIDER

COLLECTION AMOUNT: x3

RECEIVER: ID OF PROPRIETARY ORGANIZATION

PAYMENT AMOUNT: x3

D :

CREDIT SETTLEMENT

OBJECT 4

PAYER: CREDIT SETTLEMENT OBJECT 1

COLLECTION AMOUNT: -

RECEIVER: ID OF EMD SERVICE CENTER

PAYMENT AMOUNT: x4

FIG. 61

A: START CREDIT SETTLEMENT PROCESSING

S451: OBTAIN SETTLEMENT INSTITUTE OF RECEIVER FROM RECEIVER ID

S452: OBTAIN SETTLEMENT INSTITUTE OF PAYER FROM PAYER ID

S453: IS CREDIT-CHECK PROCESSING NECESSARY?

S454: EXECUTE CREDIT-CHECK PROCESSING

S455: HAS PREVIOUSLY-EXECUTED SETTLEMENT OBJECT PROCESSING ENDED?

S456: TRANSMIT SETTLEMENT INSTRUCTIONS TO SETTLEMENT INSTITUTES

S457: TRANSMIT SETTLEMENT INFORMATION TO RECEIVER

S458: TRANSMIT SETTLEMENT INFORMATION TO PAYER

S459: EXECUTE ERROR PROCESSING FOR INCOMPLETE SETTLEMENT

B: END

FIG. 62

A: START BANK SETTLEMENT PROCESSING

S471: OBTAIN SETTLEMENT INSTITUTE OF RECEIVER FROM RECEIVER ID

S472: OBTAIN SETTLEMENT INSTITUTE OF PAYER FROM PAYER ID

S473: HAS PREVIOUSLY-EXECUTED SETTLEMENT OBJECT PROCESSING ENDED?

S474: TRANSMIT SETTLEMENT INSTRUCTIONS TO SETTLEMENT INSTITUTES

S475: TRANSMIT SETTLEMENT INFORMATION TO RECEIVER

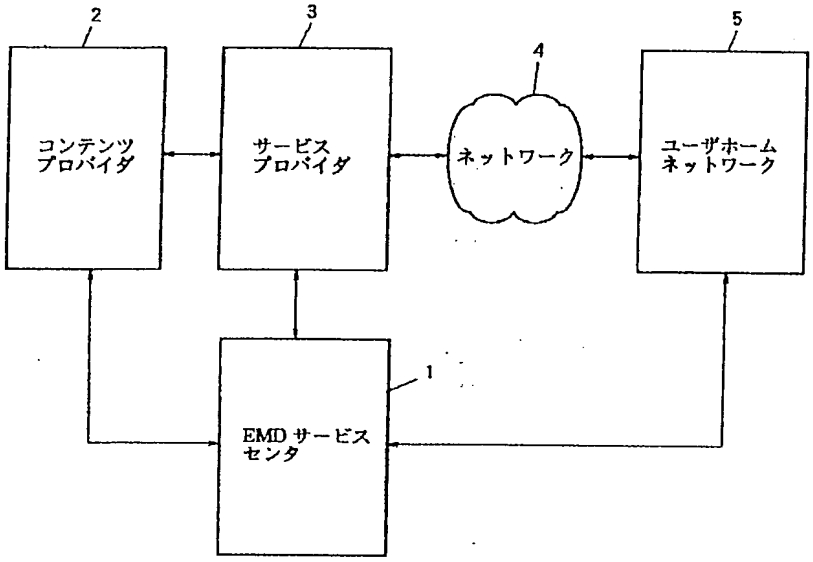
S476: TRANSMIT SETTLEMENT INFORMATION TO PAYER

S477: EXECUTE ERROR PROCESSING FOR INCOMPLETE SETTLEMENT

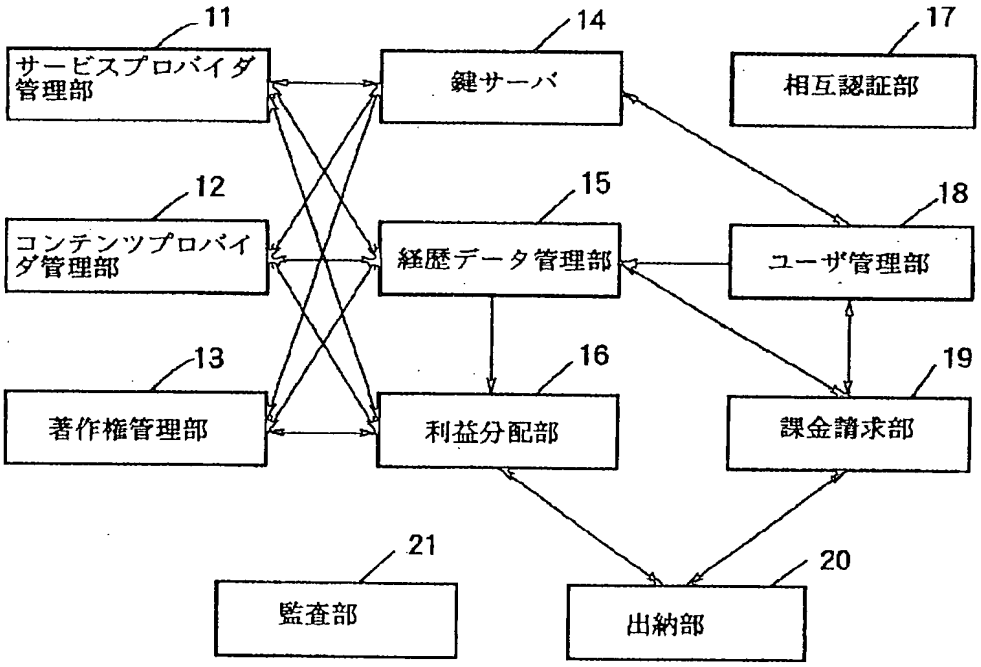
B: END

*****

【図１】

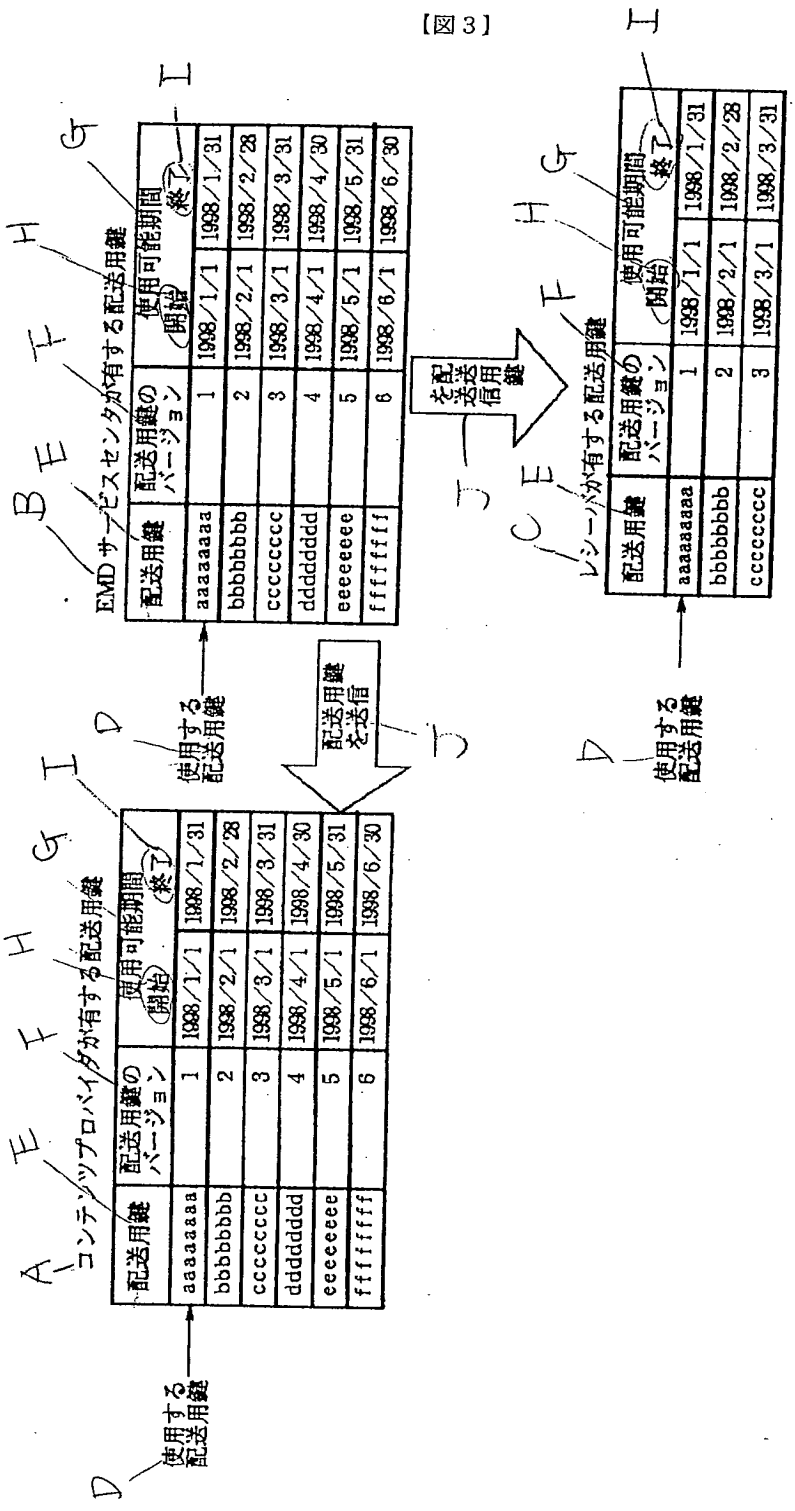


【図２】



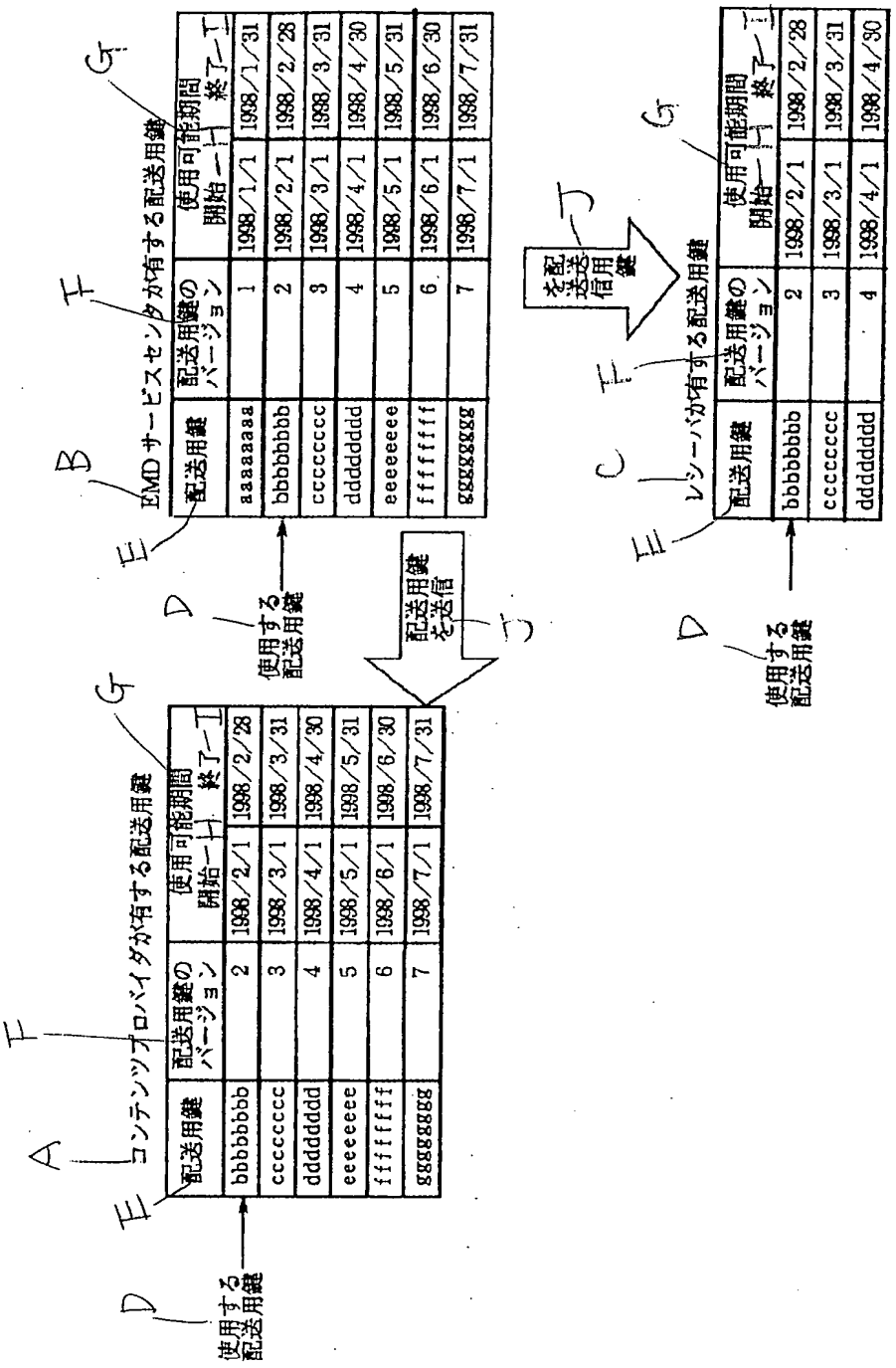
A ——EMD サービスセンタ 1

【図３】


A
B
C
D
E
F
G
H
I
J
コンテンツプロバイダが有する配送用鍵
EMDサービスセンタが有する配送用鍵
レシーバが有する配送用鍵
使用する配送用鍵
配送用鍵を送信
配送用鍵を配送信用鍵
配送用鍵
配送用鍵のバージョン
使用可能期間
開始
終了
aaaaaaaa
bbbbbbbb
cccccccc
dddddddd
eeeeeeee
ffffffff
1998/1/1
1998/2/1
1998/3/1
1998/4/1
1998/5/1
1998/6/1
1998/1/31
1998/2/28
1998/3/31
1998/4/30
1998/5/31
1998/6/30

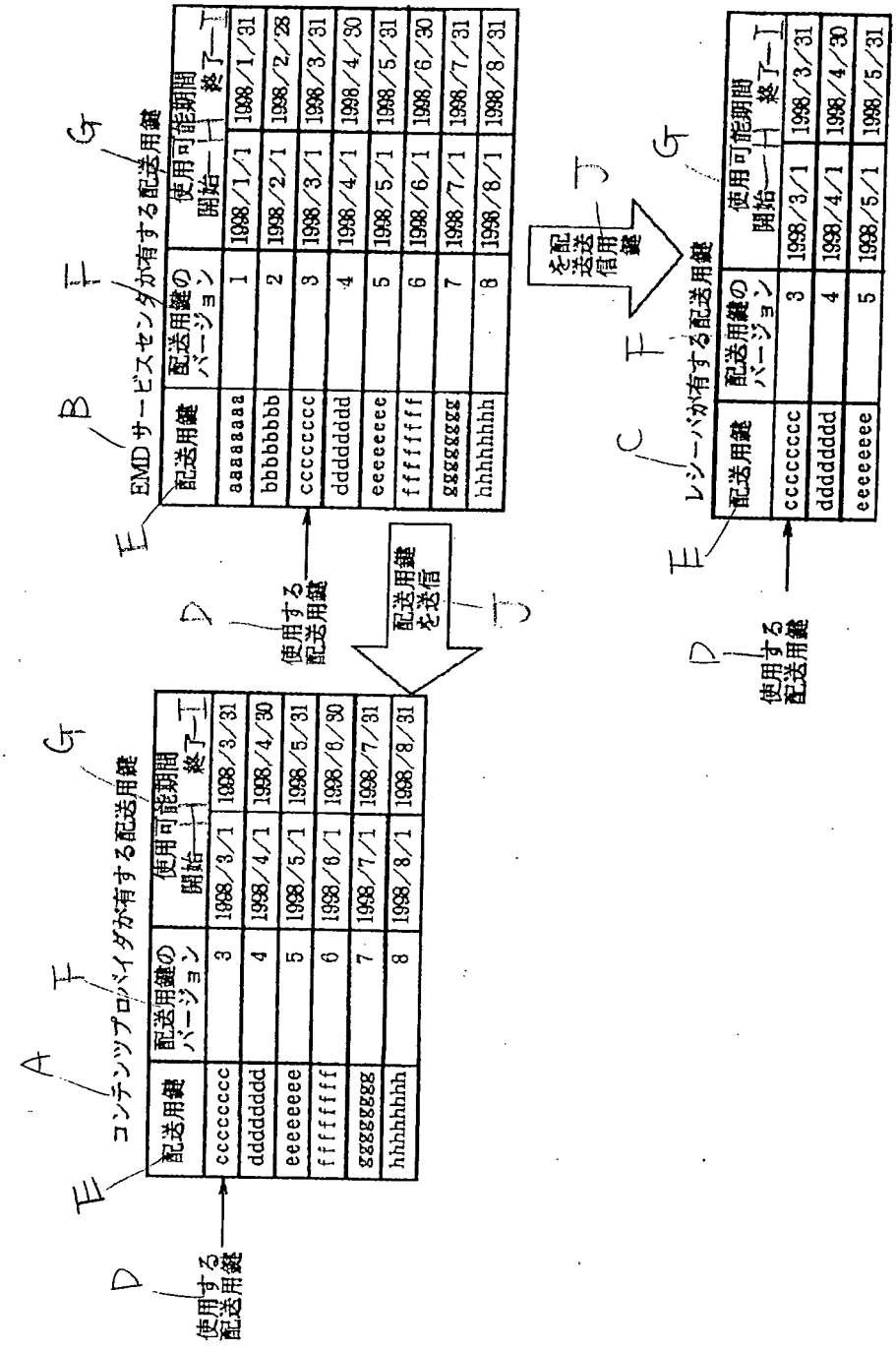
【図４】

Fig. 3 と同じ


A
B
C
D
E
F
G
コンテンツプロバイダが有する配送用鍵
IMDサービスセンタが有する配送用鍵
レシーバが有する配送用鍵
使用する配送用鍵
配送用鍵
配送用鍵のバージョン
使用可能期間 開始 終了
配送用鍵を送信
配送用鍵を送信用鍵
aaaaaaaa 1 1998/1/1 1998/1/31
bbbbbbbb 2 1998/2/1 1998/2/28
cccccccc 3 1998/3/1 1998/3/31
dddddddd 4 1998/4/1 1998/4/30
eeeeeeee 5 1998/5/1 1998/5/31
ffffffff 6 1998/6/1 1998/6/30
gggggggg 7 1998/7/1 1998/7/31

【図５】

Fig. 3 と同じ


A
B
C
D
E
F
G
コンテンツプロバイダが有する配送用鍵
EMDサービスセンタが有する配送用鍵
レシーバが有する配送用鍵
使用する配送用鍵
配送用鍵
配送用鍵のバージョン
使用可能期間
開始
終了
配送用鍵を送信
配送用鍵を配送信用鍵
ア
イ
ウ
エ
オ
カ
キ
ク
ケ
コ
サ
シ
ス
セ
ソ
タ
チ
ツ
テ
ト
ナ
ニ
ヌ
ネ
ノ
ハ
ヒ
フ
ヘ
ホ
マ
ミ
ム
メ
モ
ヤ
ユ
ヨ
ラ
リ
ル
レ
ロ
ワ
ヲ
ン

【図6】

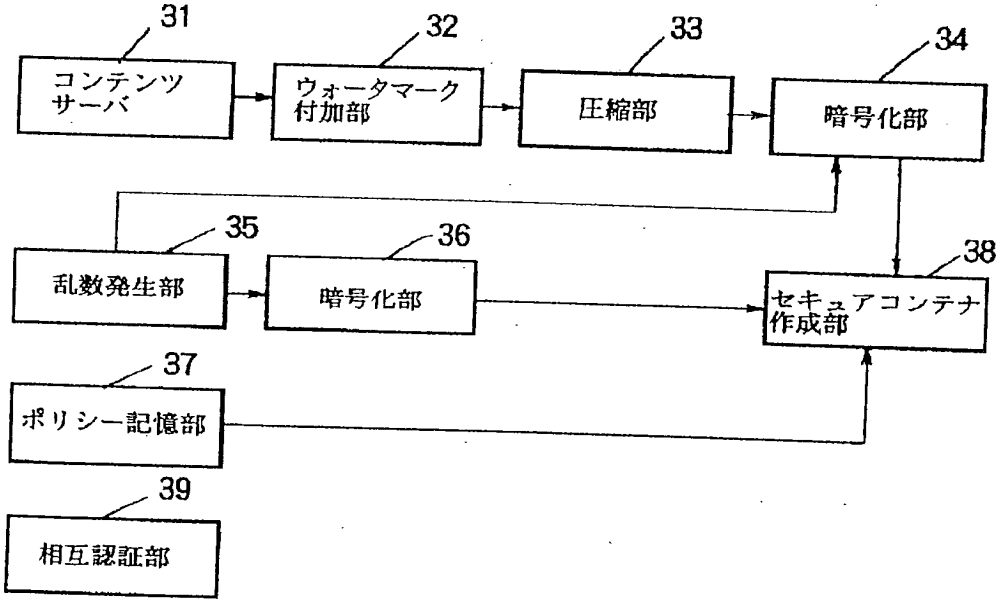
Fig. 3 と同じ

A
B
C
D
E
F
G
コンテンツプロバイダが有する配送用鍵
配送用鍵
配送用鍵のバージョン
使用可能期間
開始日
終了日
dddddddd 4 1998/4/1 1998/4/30
eeeeeeee 5 1998/5/1 1998/5/31
ffffffff 6 1998/6/1 1998/6/30
gggggggg 7 1998/7/1 1998/7/31
hhhhhhhh 8 1998/8/1 1998/8/31
iiiiiiiii 9 1998/9/1 1998/9/30
使用する配送用鍵
配送用鍵を送信
EMDサービスセンタが有する配送用鍵
aaaaaaaa 1 1998/1/1 1998/1/31
bbbbbbbb 2 1998/2/1 1998/2/28
cccccccc 3 1998/3/1 1998/3/31
dddddddd 4 1998/4/1 1998/4/30
eeeeeeee 5 1998/5/1 1998/5/31
ffffffff 6 1998/6/1 1998/6/30
gggggggg 7 1998/7/1 1998/7/31
hhhhhhhh 8 1998/8/1 1998/8/31
iiiiiiiii 9 1998/9/1 1998/9/30
使用する配送用鍵
配送用鍵を送信用鍵
レシーバが有する配送用鍵
配送用鍵
配送用鍵のバージョン
使用可能期間
開始日
終了日
dddddddd 4 1998/4/1 1998/4/30
eeeeeeee 5 1998/5/1 1998/5/31
ffffffff 6 1998/6/1 1998/6/30
使用する配送用鍵

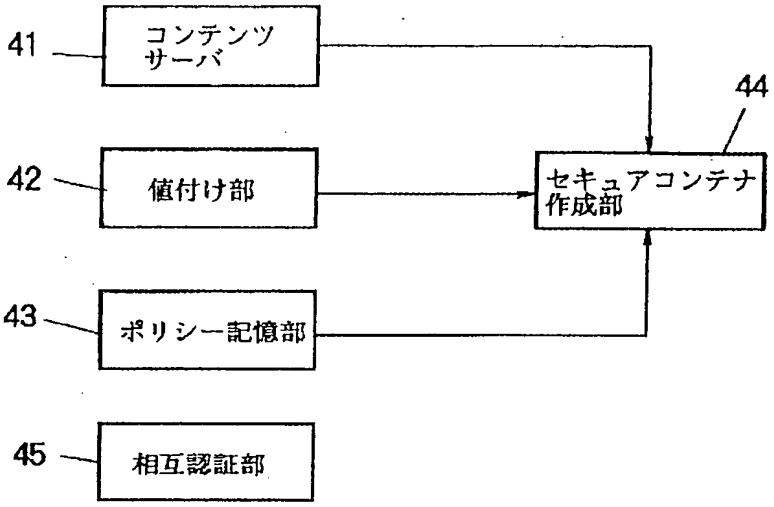
【図７】

ID	決済処理	登録	EMDサービスセンタとの接続
00000000000000001h	可	可	可
00000000000000002h	可	可	不可
00000000000000003h	可	不可	可
00000000000000004h	可	不可	不可
00000000000000005h	不可	可	可
00000000000000006h	不可	可	不可
00000000000000007h	不可	不可	可
00000000000000008h	不可	不可	不可
00000000000000009h	可	可	可
・・・			
FFFFFFFFFFFFFFEh	可	不可	不可
FFFFFFFFFFFFFFFh	不可	可	可

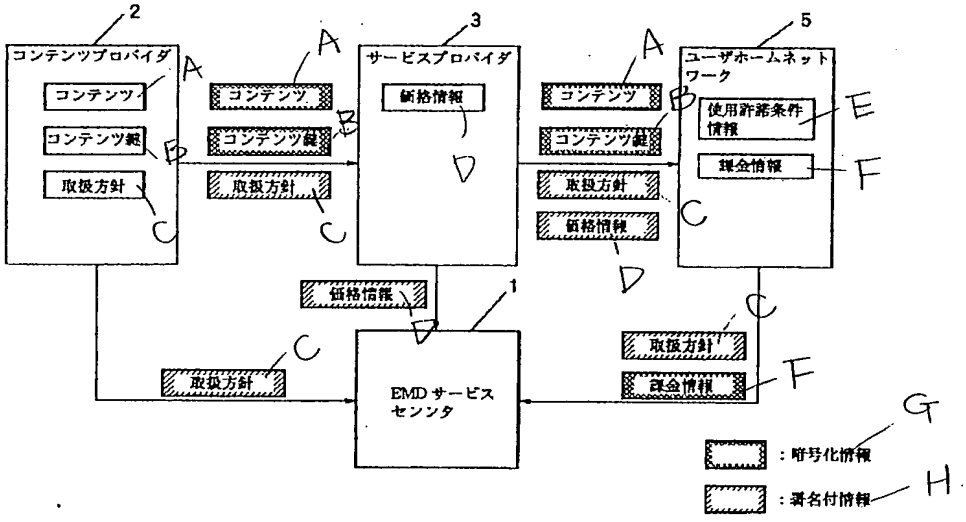
【図８】



【図９】



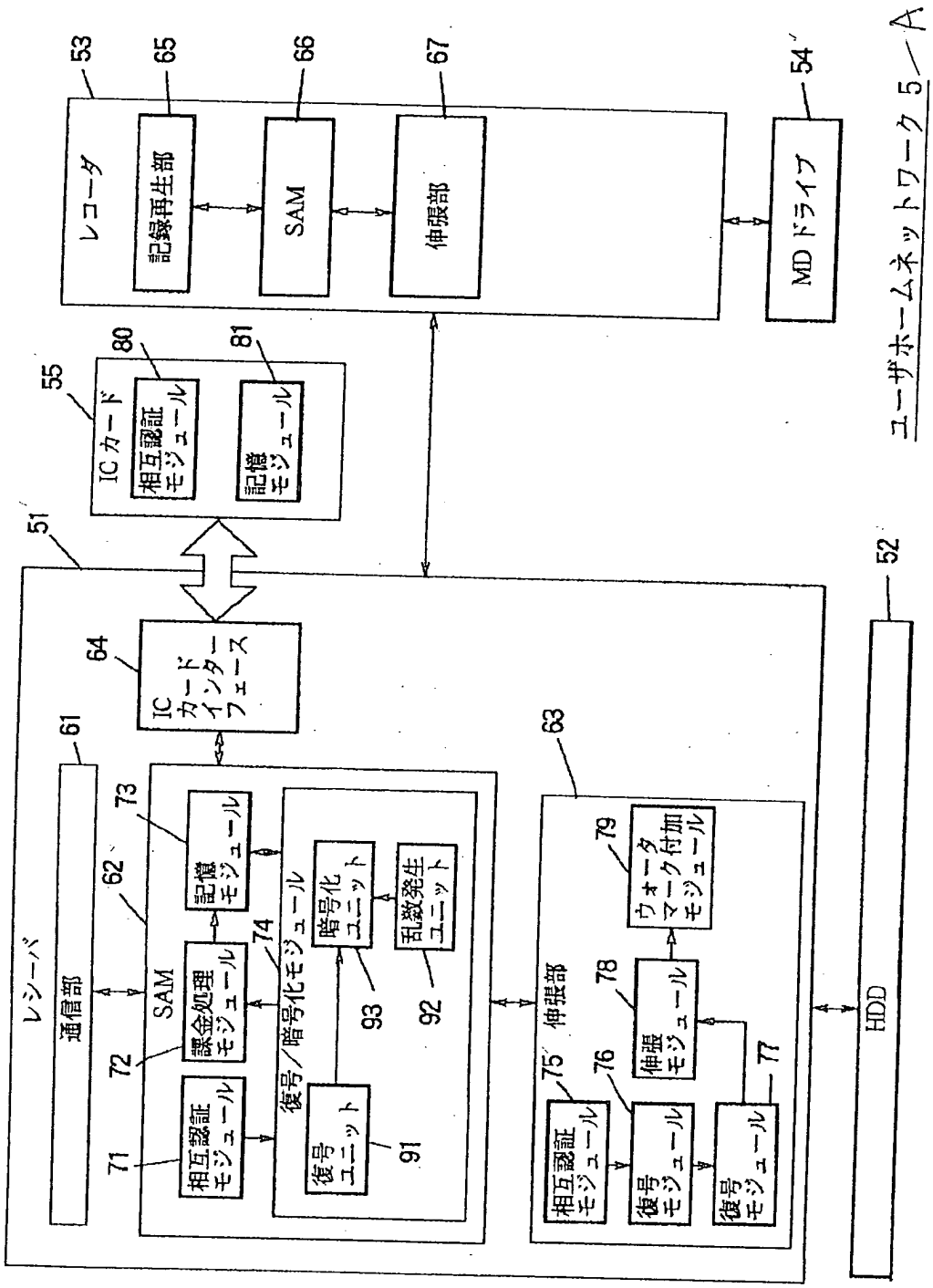
【図１２】



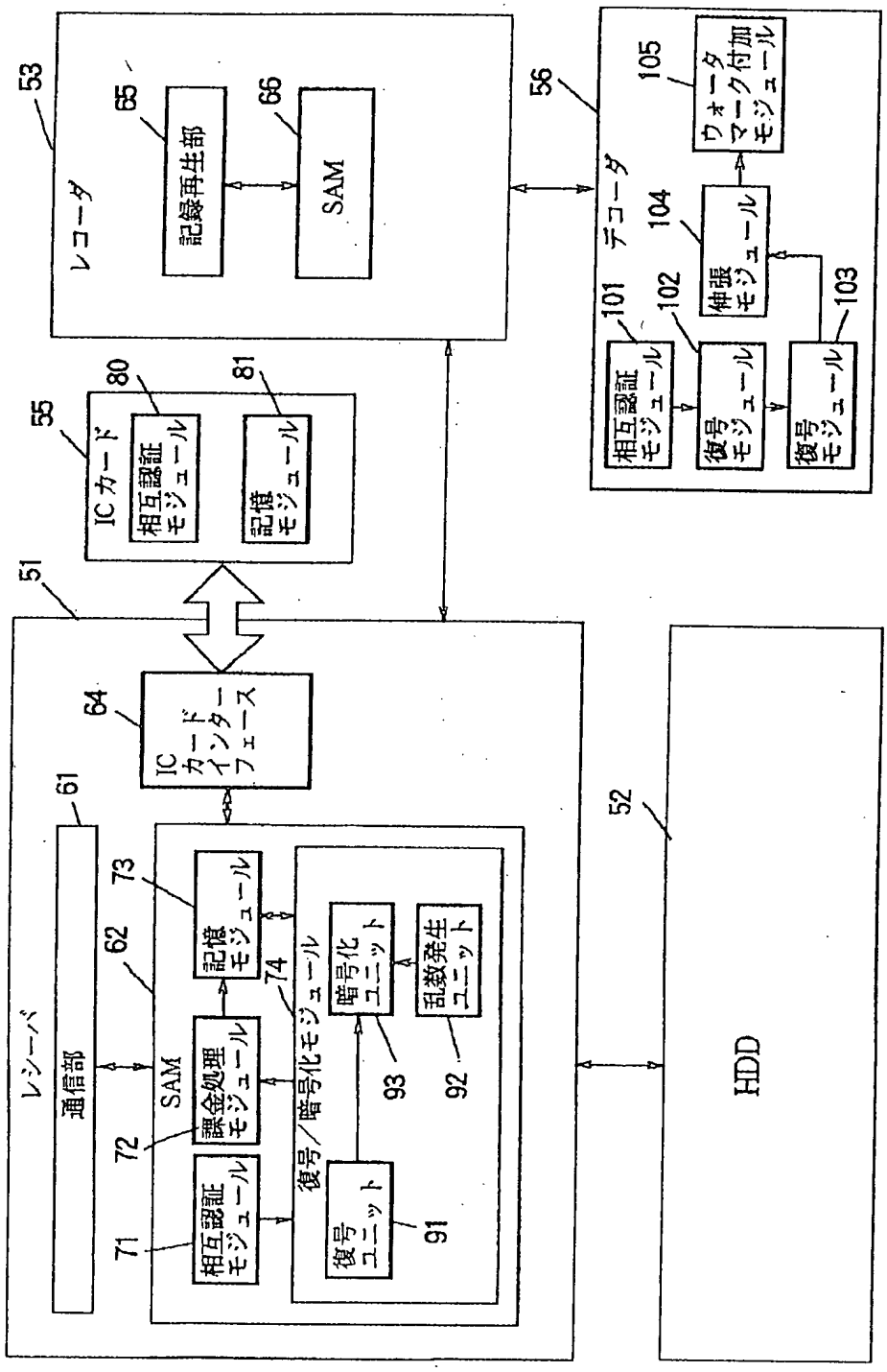
【図２８】

A コンテンツ ID	B コンテンツプロバイダ ID	C 権利団体
1	201	10%
2	201	20%

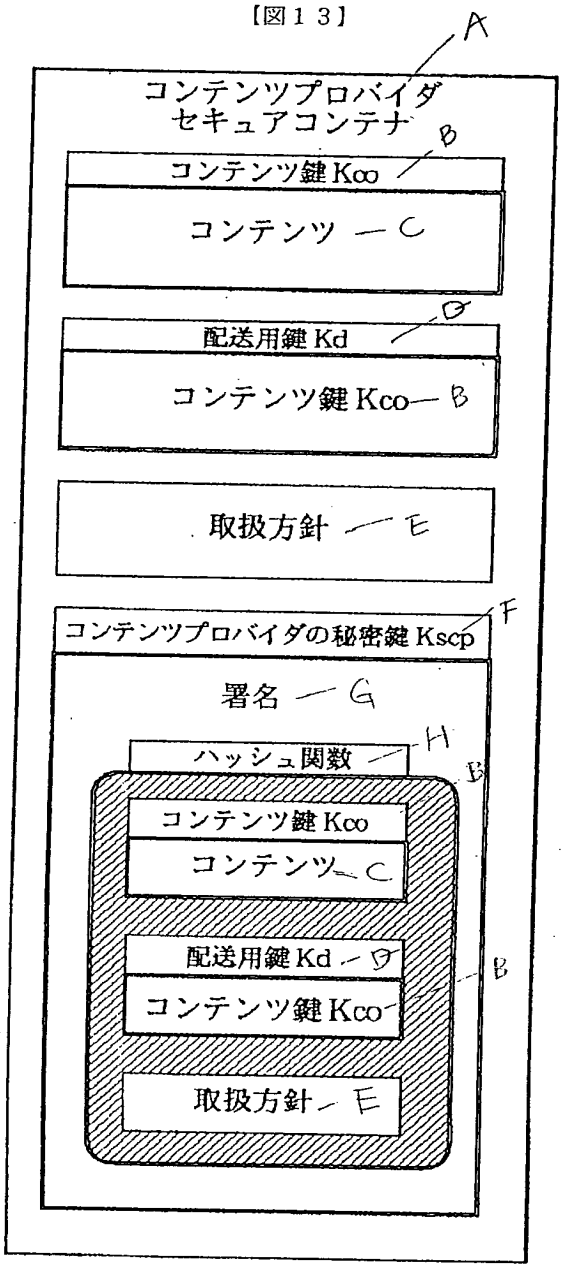
【図１０】


ユーザホームネットワーク 5
A
レコーダ
記録再生部
SAM
伸張部
MD ドライブ
ICカード
相互認証モジュール
記憶モジュール
ICカードインターフェース
レシーバ
通信部
SAM
課金処理モジュール
記憶モジュール
復号／暗号化モジュール
暗号化ユニット
乱数発生ユニット
復号ユニット
相互認証モジュール
伸張部
ウォータマーク付加モジュール
伸張モジュール
相互認証モジュール
復号モジュール
復号モジュール
HDD

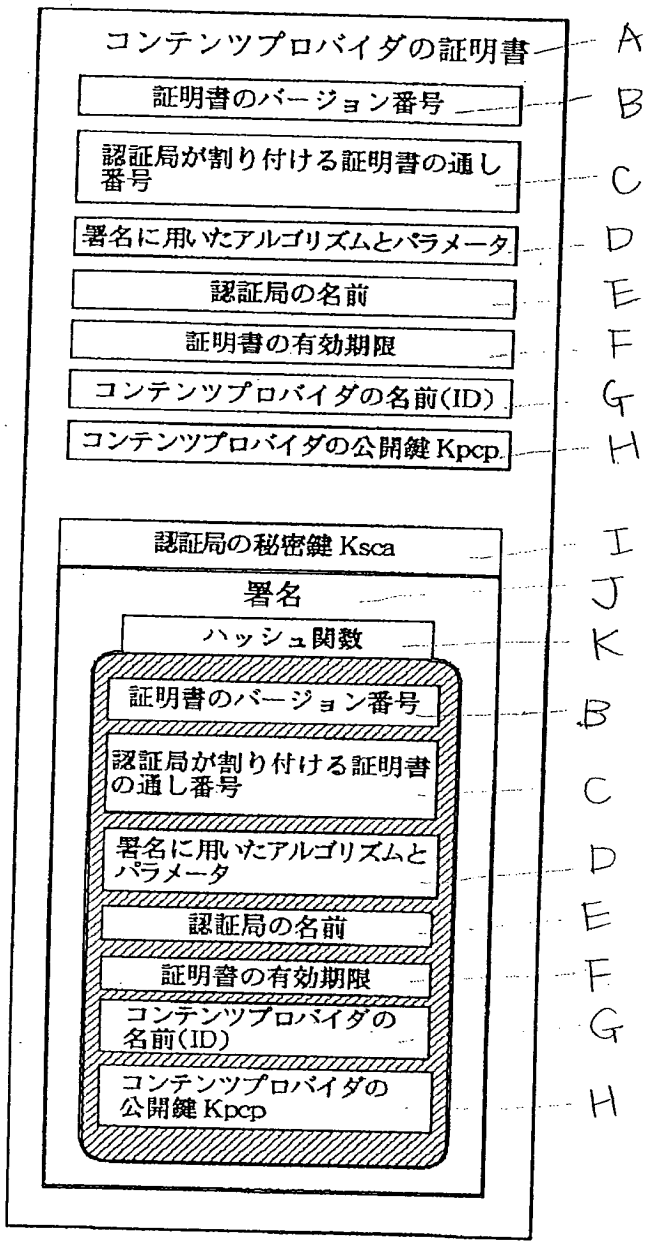
【図１１】


ユーザホームネットワーク 5
A
レコーダ
53
記録再生部
65
SAM
66
デコーダ
56
ウォータマーク付加モジュール
105
伸張モジュール
104
相互認証モジュール
101
復号モジュール
102
復号モジュール
103
ICカード
55
相互認証モジュール
80
記憶モジュール
81
51
ICカードインターフェース
64
レシーバ
61
通信部
62
SAM
相互認証モジュール
71
課金処理モジュール
72
記憶モジュール
73
74
復号／暗号化モジュール
復号ユニット
91
暗号化ユニット
93
乱数発生ユニット
92
52
HDD

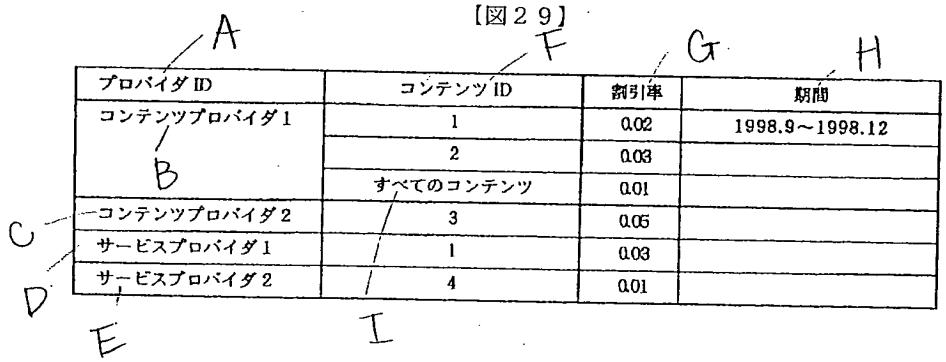
【図１３】



【図１４】

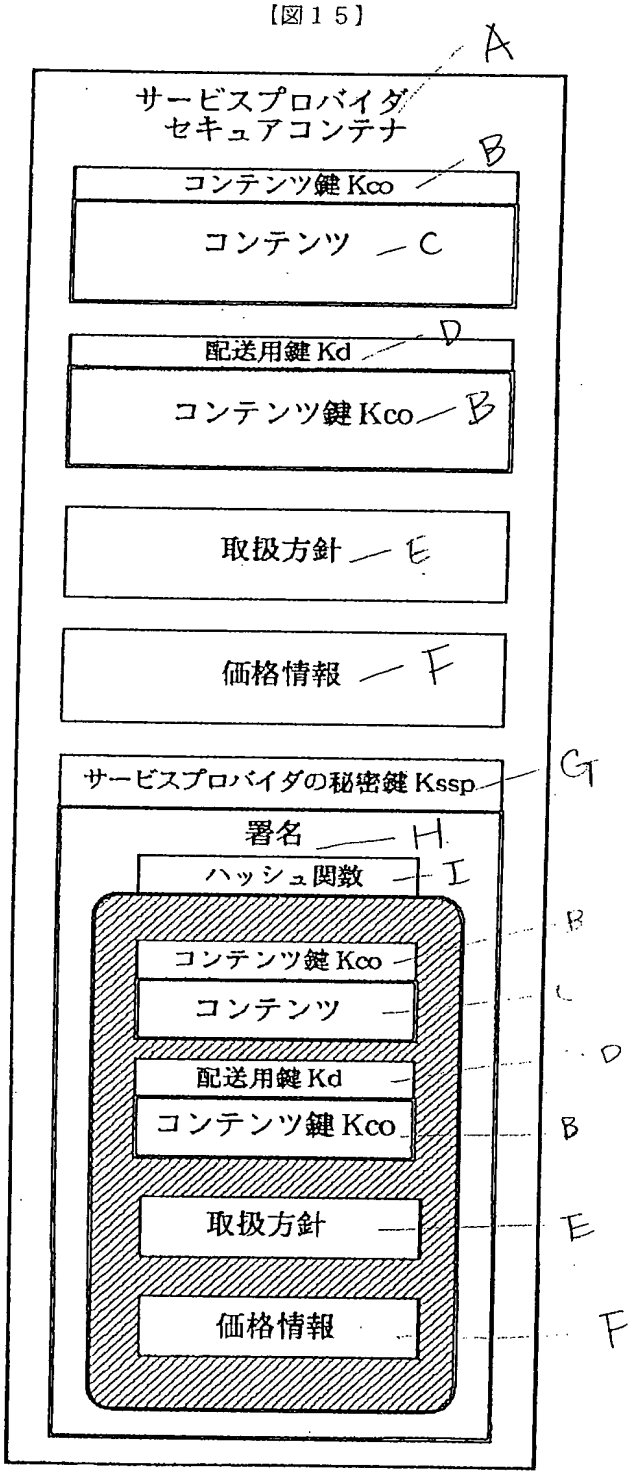


【図２９】

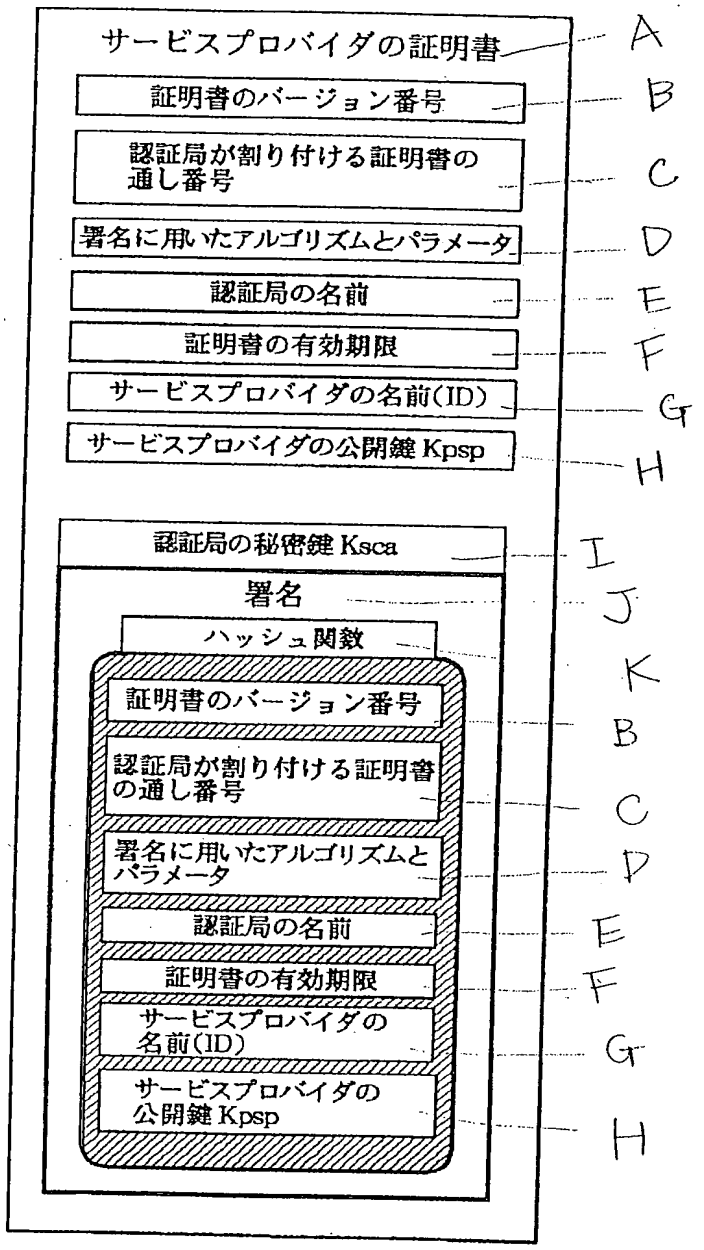


プロバイダ ID	コンテンツ ID	割引率	期間
コンテンツプロバイダ１	1	0.02	1998.9～1998.12
	2	0.03	
	すべてのコンテンツ	0.01	
コンテンツプロバイダ２	3	0.05	
サービスプロバイダ１	1	0.03	
サービスプロバイダ２	4	0.01	

【図１５】



【図１６】



【図３０】

月額固定額	変動額		
1000円	期間	1998. 8.～1998. 9	－10%
	利用料	3000円以上	－5%

A　B　C　D　E　F

【図１７】

(A)　取扱方針

利用内容	再生	シングルコピー	マルチコピー
可／否	1	0	1

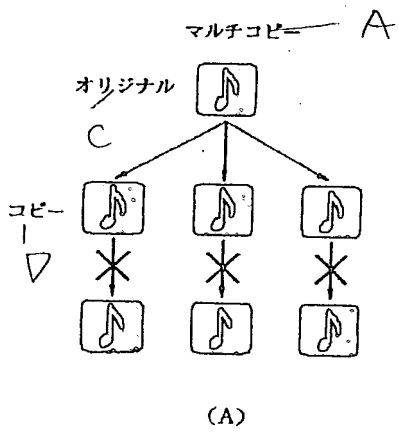
(B)　取扱方針および価格情報

利用内容	再生	シングルコピー	マルチコピー
可／否	1	0	1
価格	150円	－	80円

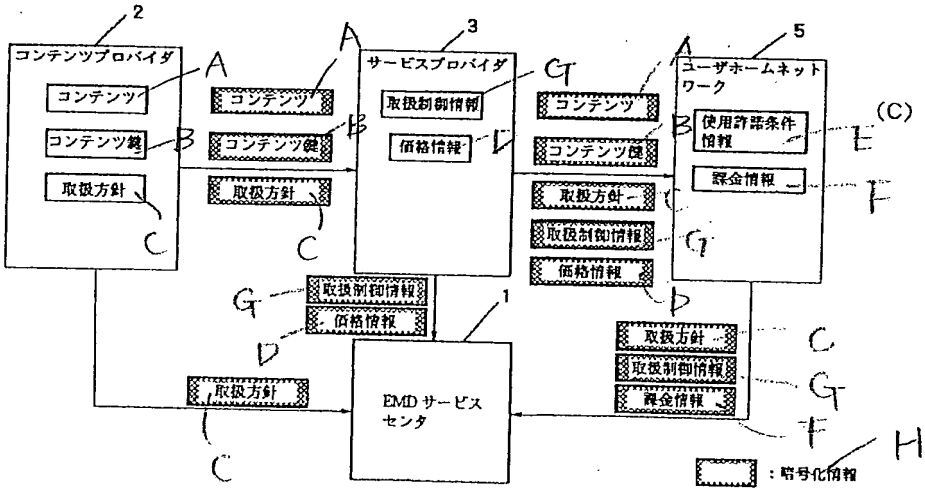
(C)　使用許諾条件情報

利用内容	再生	シングルコピー	マルチコピー
可／否	1	0	0

【図１８】



【図２４】



【図５８】

(A)
クレジット決済オブジェクト１
支払元：ユーザの ID
徴収額：x
支払先：サービスプロバイダの ID
支払額：x1

(B)
クレジット決済オブジェクト２
支払元：クレジット決済オブジェクト１
徴収額：－
支払先：コンテンツプロバイダの ID
支払額：x2

(C)
クレジット決済オブジェクト３
支払元：クレジット決済オブジェクト１
徴収額：－
支払先：権利団体の ID
支払額：x3

(D)
クレジット決済オブジェクト４
支払元：クレジット決済オブジェクト１
徴収額：－
支払先：EMD サービスセンタの ID
支払額：x4

【図５９】

(A)
銀行決済オブジェクト１
支払元：サービスプロバイダの ID
徴収額：y1
支払先：EMD サービスセンタの ID
支払額：y1

(B)
銀行決済オブジェクト２
支払元：コンテンツプロバイダの ID
徴収額：y2
支払先：EMD サービスセンタの ID
支払額：y2

(C)
銀行決済オブジェクト３
支払元：権利団体の ID
徴収額：y3
支払先：EMD サービスセンタの ID
支払額：y3

【図１９】

(A) 取扱方針 利益分配

利用内容	再生	シングルコピー	マルチコピー
可／否	1	0	1
利益分配	70円	－	40円

(B) 取扱方針 利益分配 価格情報

利用内容	再生	シングルコピー	マルチコピー
可／否	1	0	1
利益分配	60円	－	30円
分配価格	150円	－	80円

(C) 課金情報

利用内容	再生	シングルコピー	マルチコピー
利用回数	1	0	0

【図２０】

(A) 取扱方針 および 価格情報

利用内容	再生		
	制限なし	回数制限	期日制限
	－	5	1998／12／31
価格	－	60円	80円

(B) 使用許諾条件情報

利用内容	再生		
	制限なし	回数制限	期日制限
	1	5	－

3回再生後

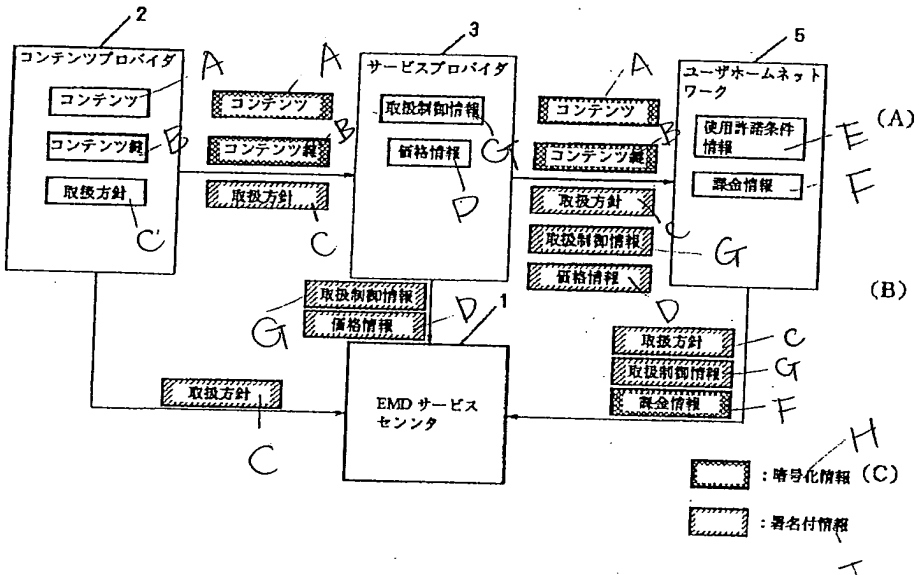
(C) 使用許諾条件情報

利用内容	再生		
	制限なし	回数制限	期日制限
	－	2	－

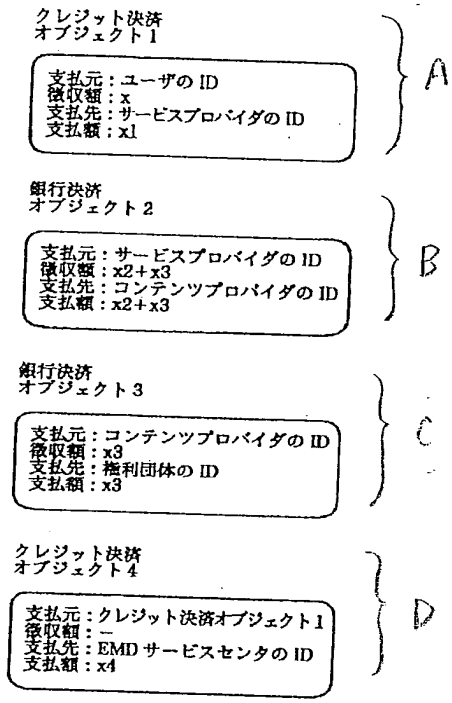
【図４２】

SAMのID (64bit)	登録拒絶フラグ (1bit)	ステータスフラグ (4bit)	コンディションフラグ (1bit)	署名
0000000000000001h	1	0000	0	xxxxxxxxxx
0000000000000002h	1	1010	1	xxxxxxxxxx
0000000000000003h	1	1100	1	xxxxxxxxxx
000000000000000Ah	0	0000	1	xxxxxxxxxx

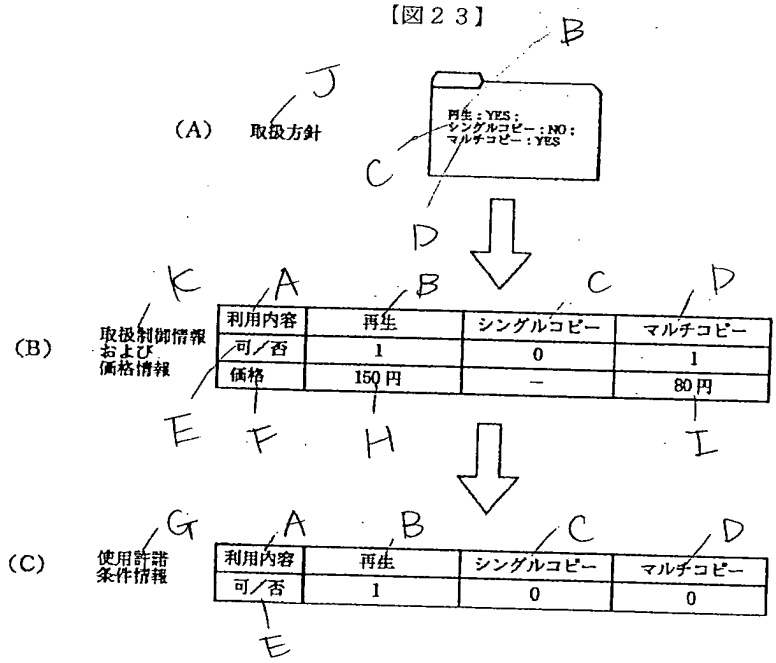
【図２１】


2
コンテンツプロバイダ
コンテンツ
コンテンツ鍵
取扱方針
3
サービスプロバイダ
取扱制御情報
価格情報
5
ユーザホームネットワーク
使用許諾条件情報
課金情報
(A)
(B)
EMD サービスセンタ
1
：暗号化情報 (C)
：署名付情報

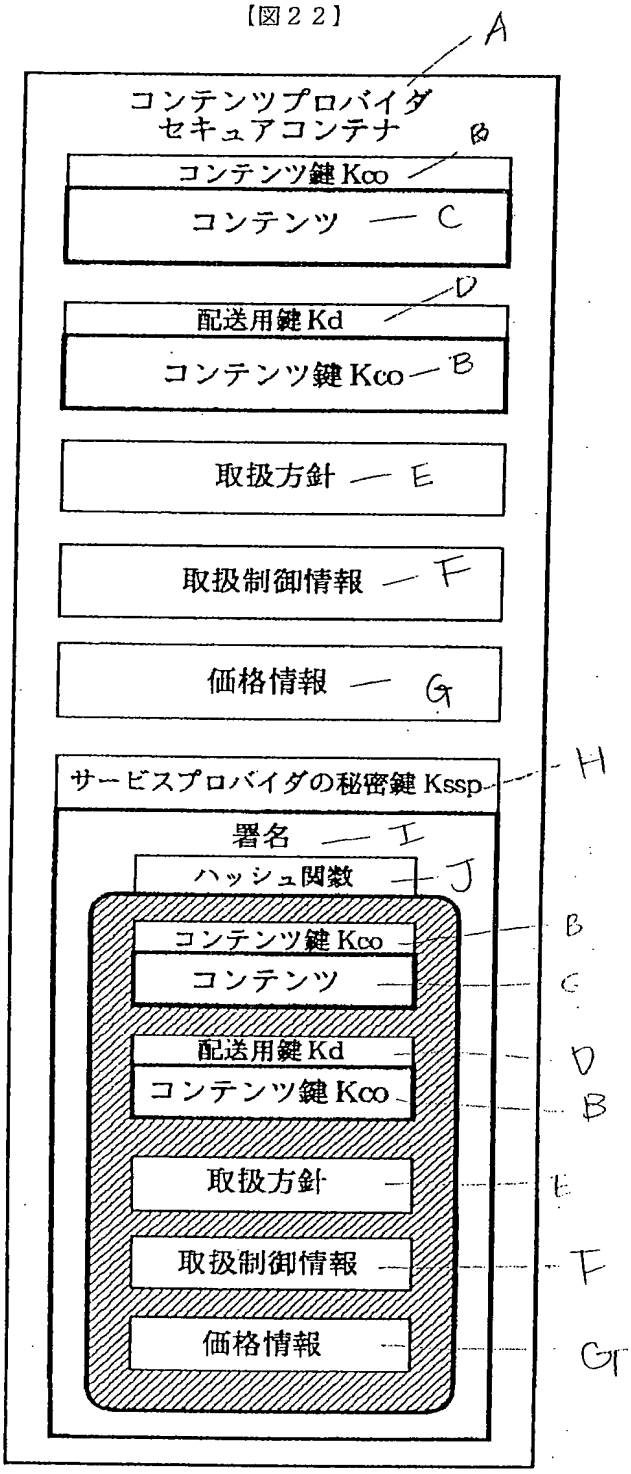
【図６０】


クレジット決済
オブジェクト１
支払元：ユーザの ID
徴収額：x
支払先：サービスプロバイダの ID
支払額：x1
A
銀行決済
オブジェクト２
支払元：サービスプロバイダの ID
徴収額：x2+x3
支払先：コンテンツプロバイダの ID
支払額：x2+x3
B
銀行決済
オブジェクト３
支払元：コンテンツプロバイダの ID
徴収額：x3
支払先：権利団体の ID
支払額：x3
C
クレジット決済
オブジェクト４
支払元：クレジット決済オブジェクト１
徴収額：－
支払先：EMD サービスセンタの ID
支払額：x4
(D)
D

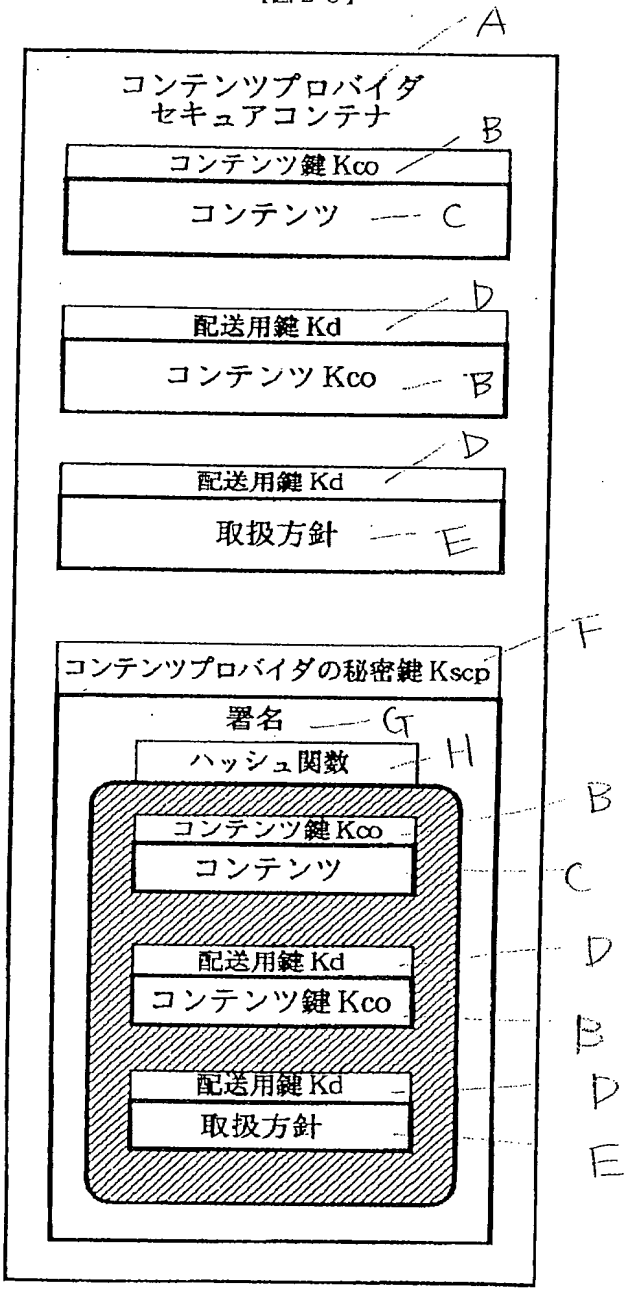
【図２３】


(A) 取扱方針
再生：YES；
シングルコピー：NO；
マルチコピー：YES
(B) 取扱制御情報および価格情報
利用内容 | 再生 | シングルコピー | マルチコピー
可／否 | 1 | 0 | 1
価格 | 150 円 | － | 80 円
(C) 使用許諾条件情報
利用内容 | 再生 | シングルコピー | マルチコピー
可／否 | 1 | 0 | 0

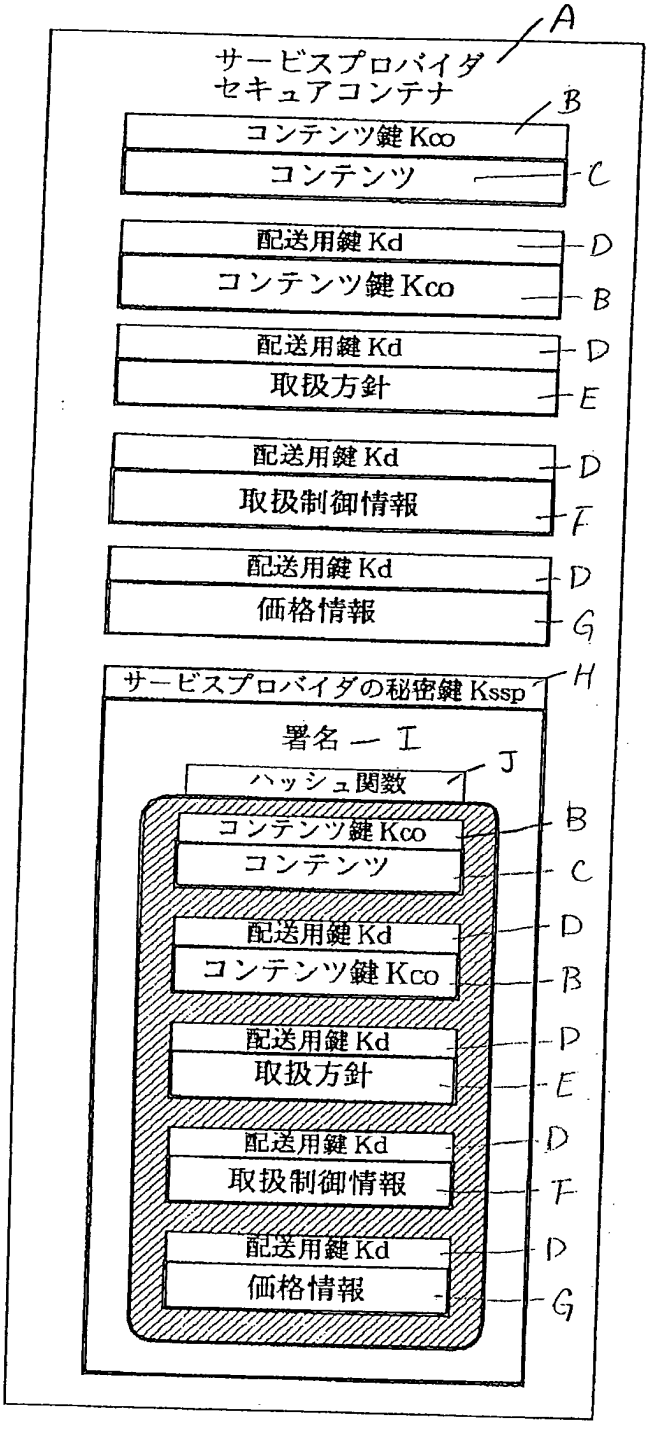
【図２２】


A
コンテンツプロバイダ
セキュアコンテナ
B
コンテンツ鍵 Kco
コンテンツ
C
D
配送用鍵 Kd
コンテンツ鍵 Kco
B
取扱方針
E
取扱制御情報
F
価格情報
G
サービスプロバイダの秘密鍵 Kssp
H
署名
I
ハッシュ関数
J
コンテンツ鍵 Kco
B
コンテンツ
C
配送用鍵 Kd
D
コンテンツ鍵 Kco
B
取扱方針
E
取扱制御情報
F
価格情報
G

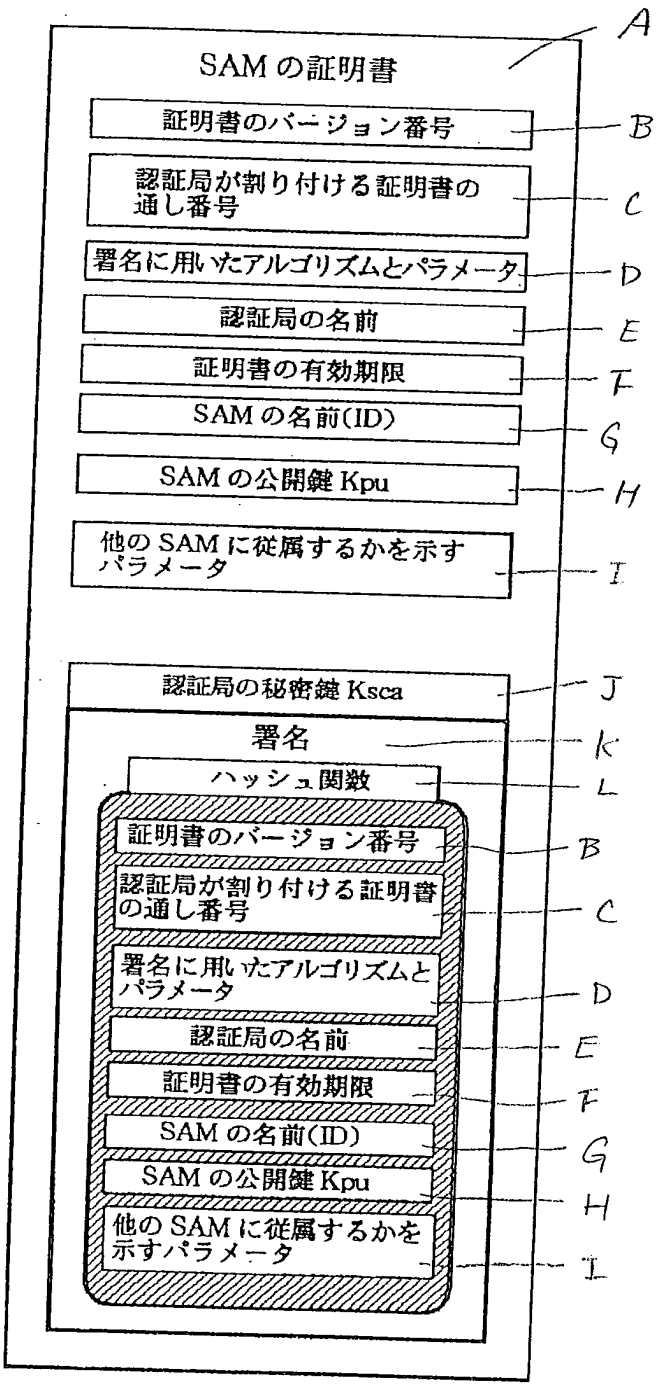
【図２５】


A
コンテンツプロバイダ
セキュアコンテナ
B
コンテンツ鍵 Kco
コンテンツ
C
D
配送用鍵 Kd
コンテンツ Kco
B
配送用鍵 Kd
取扱方針
E
F
コンテンツプロバイダの秘密鍵 Kscp
署名
G
ハッシュ関数
H
コンテンツ鍵 Kco
コンテンツ
配送用鍵 Kd
コンテンツ鍵 Kco
配送用鍵 Kd
取扱方針
B
C
D
B
D
E

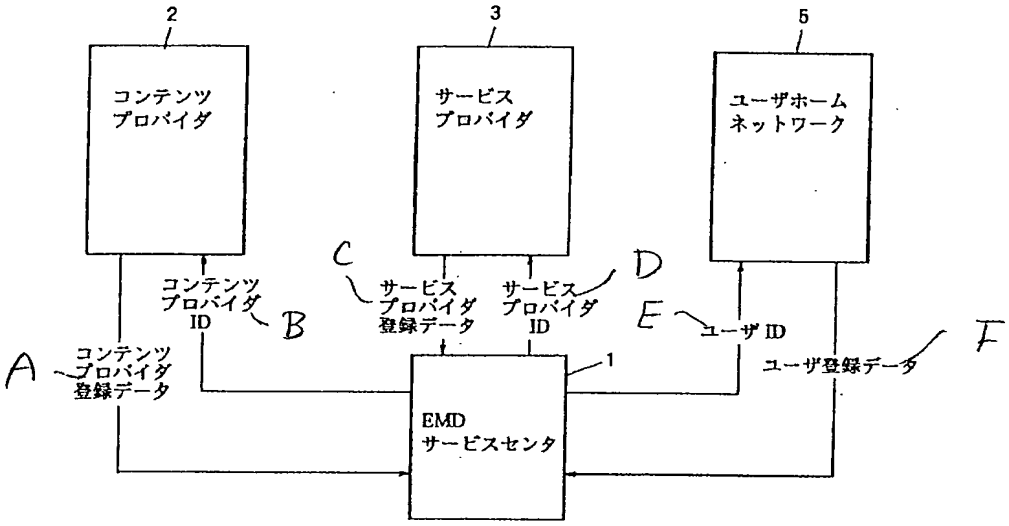
【図２６】


A
サービスプロバイダ
セキュアコンテナ
B
コンテンツ鍵 Kco
C
コンテンツ
D
配送用鍵 Kd
B
コンテンツ鍵 Kco
D
配送用鍵 Kd
E
取扱方針
D
配送用鍵 Kd
F
取扱制御情報
D
配送用鍵 Kd
G
価格情報
H
サービスプロバイダの秘密鍵 Kssp
署名－Ｉ
J
ハッシュ関数
B
コンテンツ鍵 Kco
C
コンテンツ
D
配送用鍵 Kd
B
コンテンツ鍵 Kco
D
配送用鍵 Kd
E
取扱方針
D
配送用鍵 Kd
F
取扱制御情報
D
配送用鍵 Kd
G
価格情報

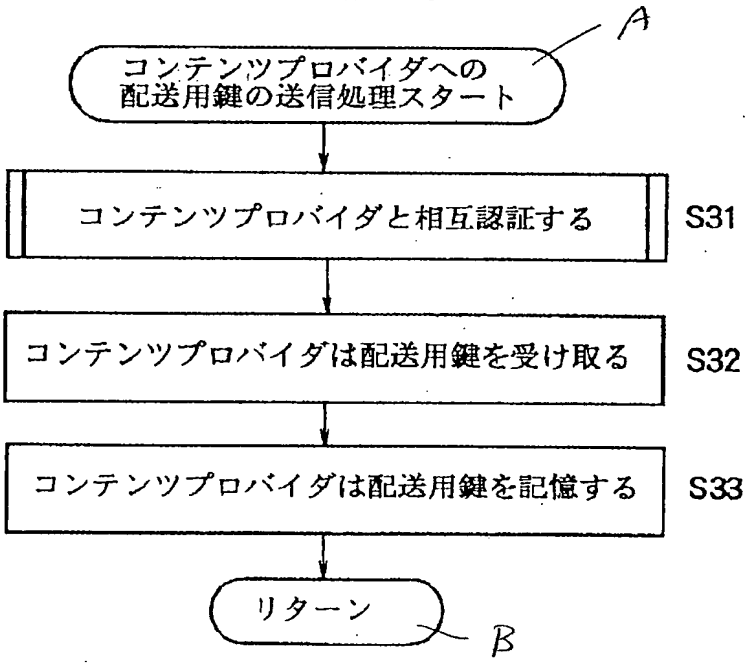
【図４１】


A
SAM の証明書
証明書のバージョン番号
B
認証局が割り付ける証明書の通し番号
C
署名に用いたアルゴリズムとパラメータ
D
認証局の名前
E
証明書の有効期限
F
SAM の名前(ID)
G
SAM の公開鍵 Kpu
H
他の SAM に従属するかを示すパラメータ
I
認証局の秘密鍵 Ksca
J
署名
K
ハッシュ関数
L
証明書のバージョン番号
B
認証局が割り付ける証明書の通し番号
C
署名に用いたアルゴリズムとパラメータ
D
認証局の名前
E
証明書の有効期限
F
SAM の名前(ID)
G
SAM の公開鍵 Kpu
H
他の SAM に従属するかを示すパラメータ
I

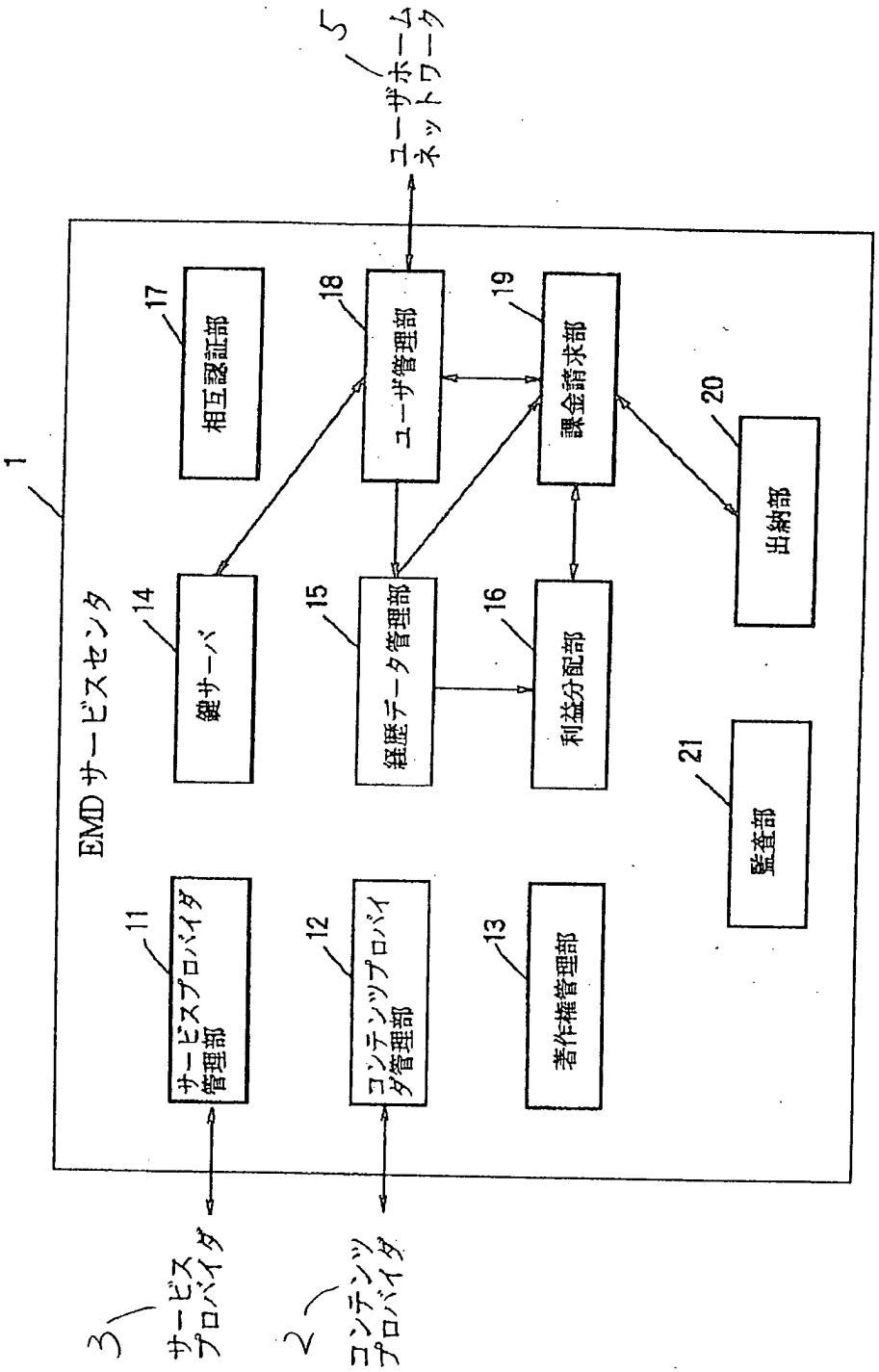
【図２７】


2
3
5
コンテンツ
プロバイダ
サービス
プロバイダ
ユーザホーム
ネットワーク
C
D
E
コンテンツ
プロバイダ
ID
B
サービス
プロバイダ
登録データ
サービス
プロバイダ
ID
ユーザ ID
A
コンテンツ
プロバイダ
登録データ
1
ユーザ登録データ
F
EMD
サービスセンタ

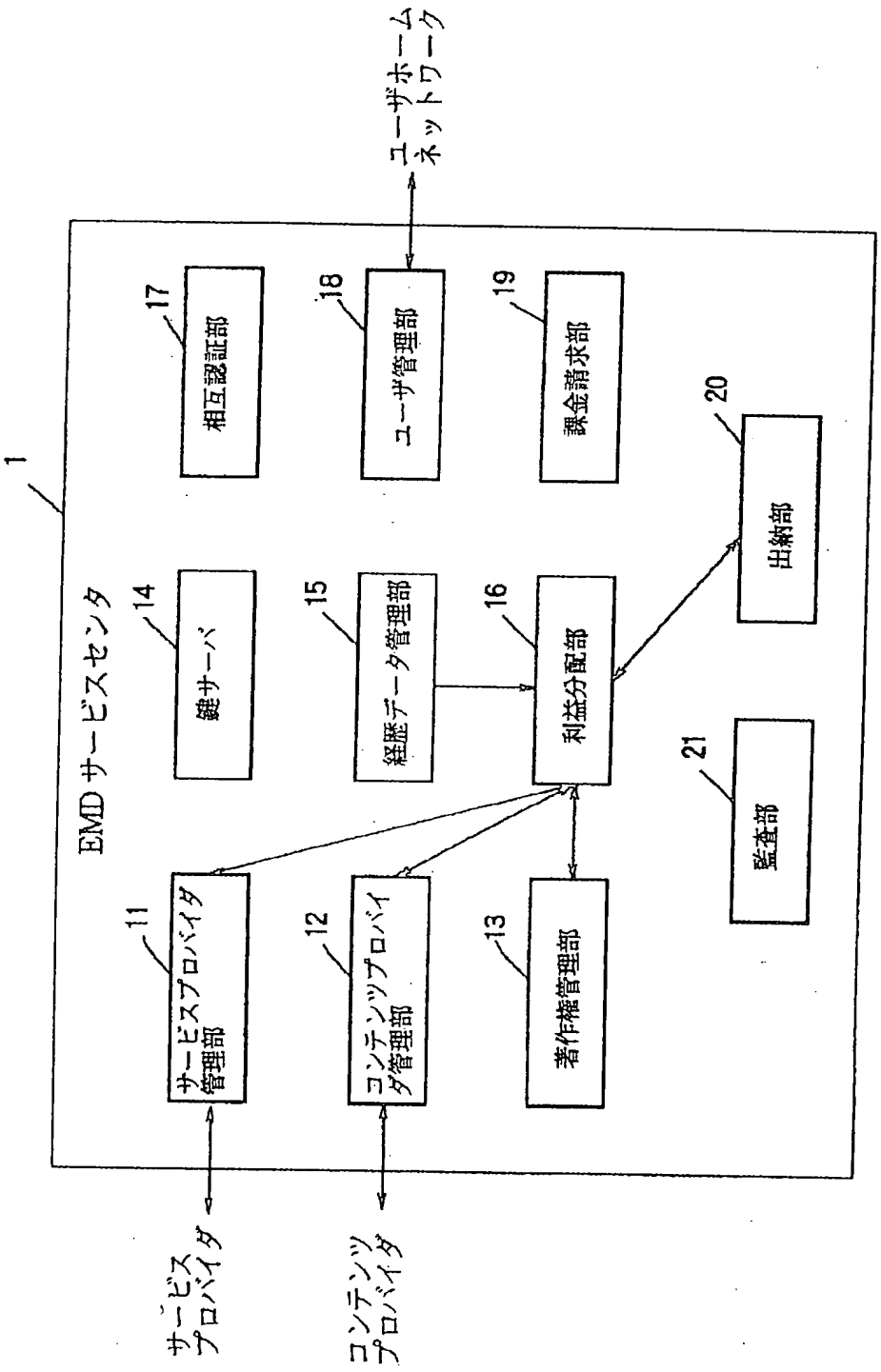
【図３６】


A
コンテンツプロバイダへの
配送用鍵の送信処理スタート
コンテンツプロバイダと相互認証する
S31
コンテンツプロバイダは配送用鍵を受け取る
S32
コンテンツプロバイダは配送用鍵を記憶する
S33
リターン
B

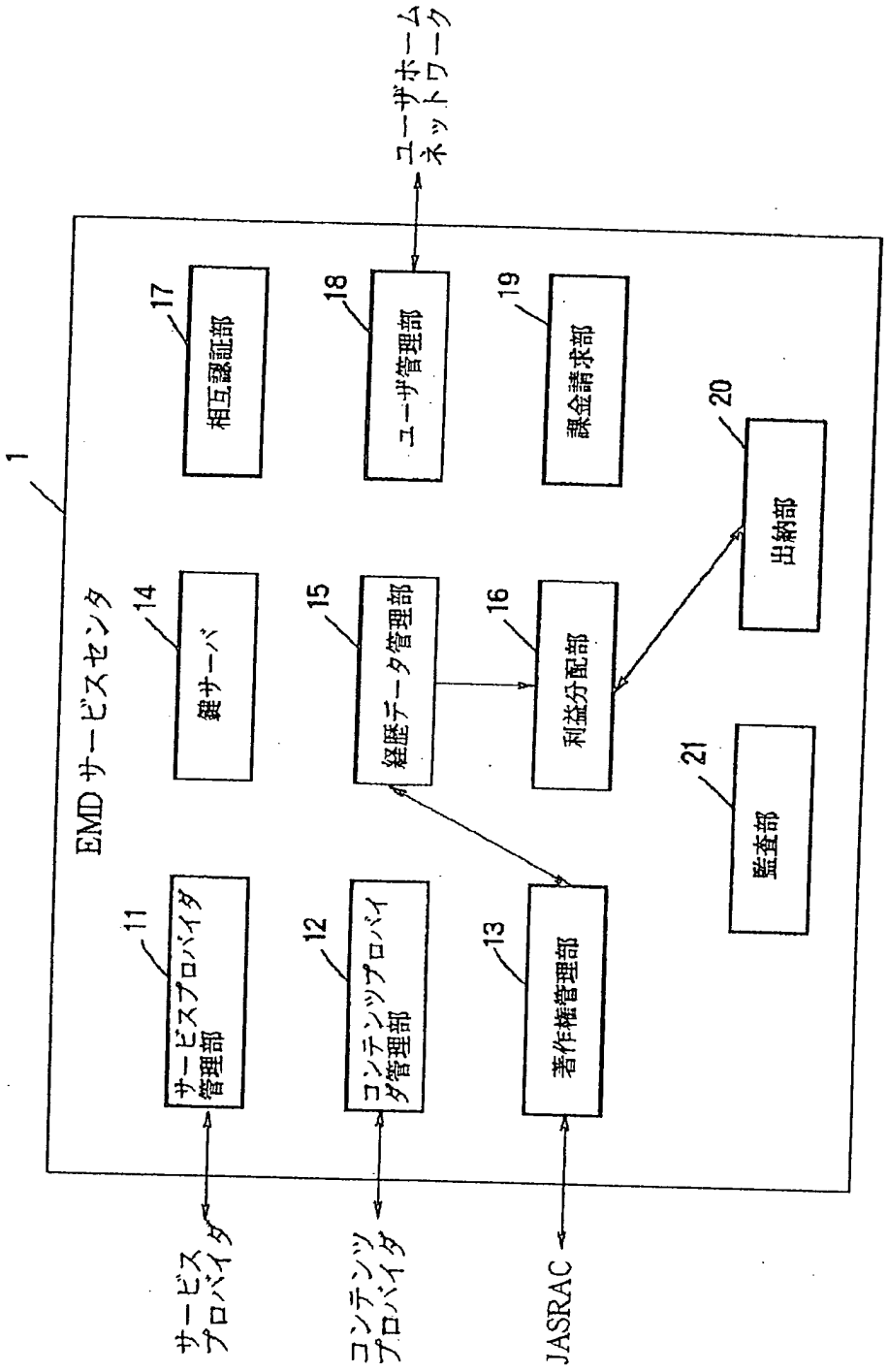
【図３１】


5
ユーザホームネットワーク
1
EMDサービスセンタ
17
相互認証部
18
ユーザ管理部
19
課金請求部
20
出納部
14
鍵サーバ
15
経歴データ管理部
16
利益分配部
21
監査部
11
サービスプロバイダ管理部
12
コンテンツプロバイダ管理部
13
著作権管理部
3
サービスプロバイダ
2
コンテンツプロバイダ

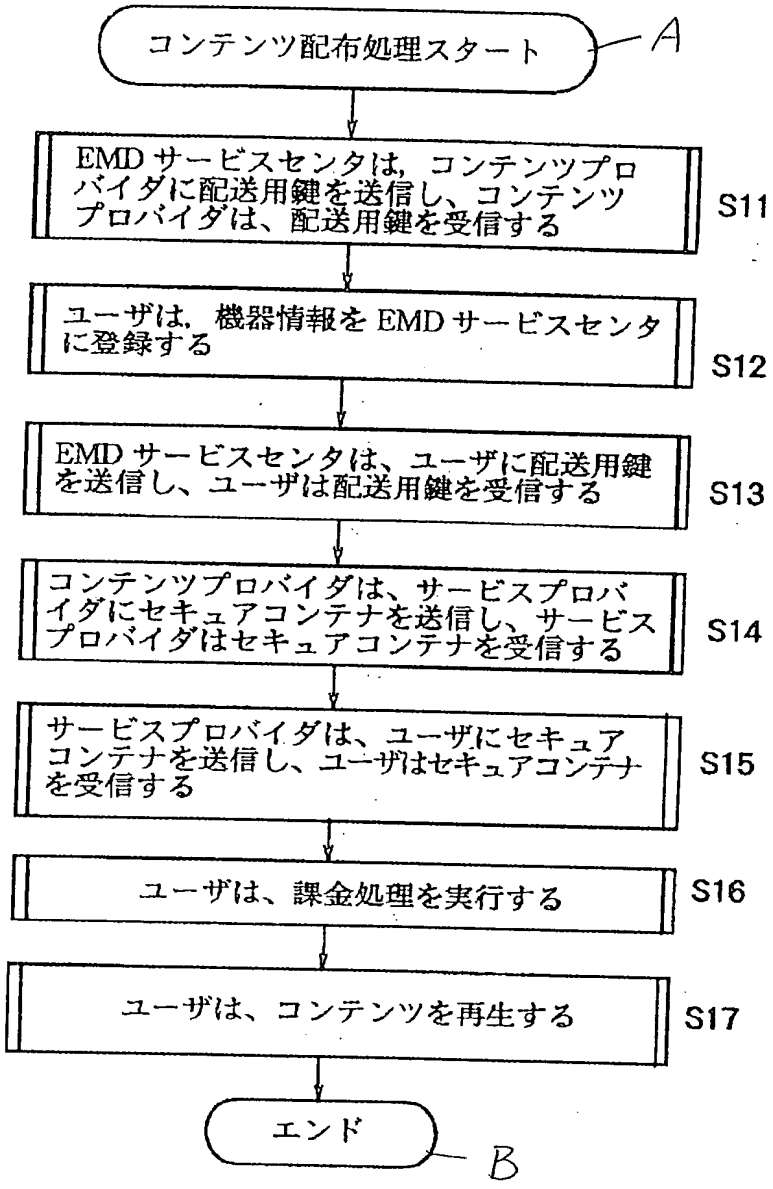
【図３２】


ユーザホームネットワーク
EMDサービスセンタ
1
相互認証部
17
ユーザ管理部
18
課金請求部
19
出納部
20
鍵サーバ
14
経歴データ管理部
15
利益分配部
16
監査部
21
サービスプロバイダ管理部
11
コンテンツプロバイダ管理部
12
著作権管理部
13
サービスプロバイダ
コンテンツプロバイダ

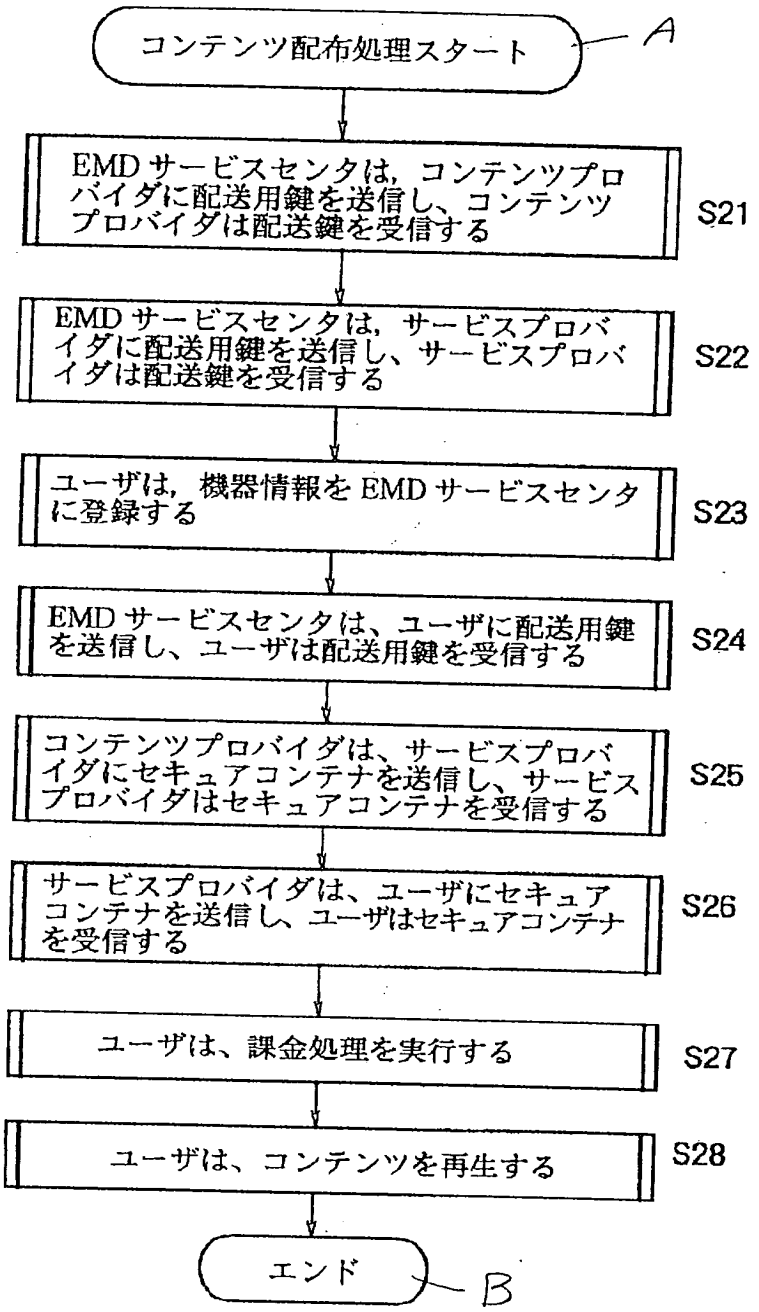
【図３３】


ユーザホーム
ネットワーク
1
EMD サービスセンタ
17
相互認証部
18
ユーザ管理部
19
課金請求部
20
出納部
14
鍵サーバ
15
経歴データ管理部
16
利益分配部
21
監査部
11
サービスプロバイダ
管理部
12
コンテンツプロバイ
ダ管理部
13
著作権管理部
サービス
プロバイダ
コンテンツ
プロバイダ
JASRAC

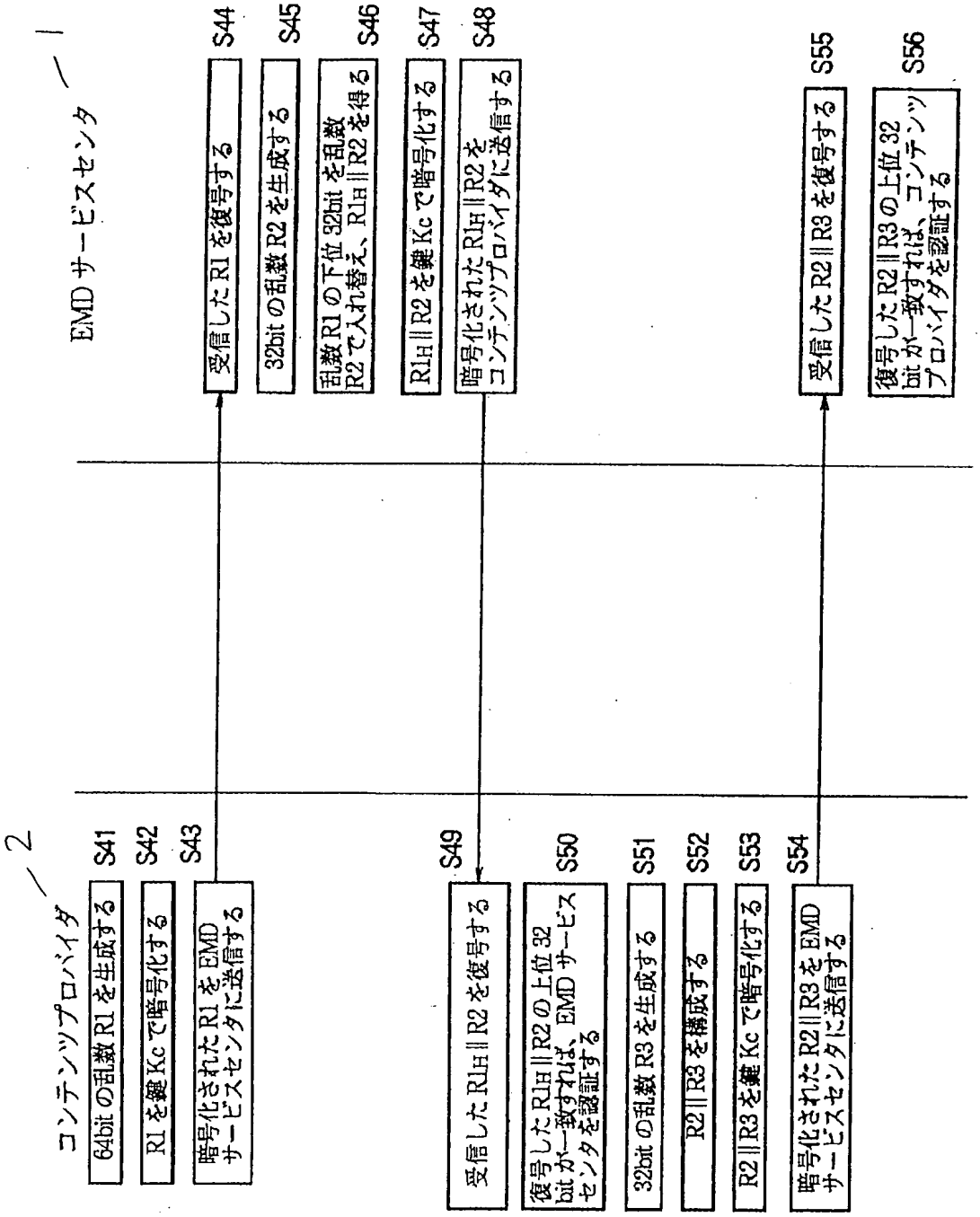
【図３４】


コンテンツ配布処理スタート
A
EMD サービスセンタは，コンテンツプロバイダに配送用鍵を送信し、コンテンツプロバイダは、配送用鍵を受信する
S11
ユーザは，機器情報を EMD サービスセンタに登録する
S12
EMD サービスセンタは、ユーザに配送用鍵を送信し、ユーザは配送用鍵を受信する
S13
コンテンツプロバイダは、サービスプロバイダにセキュアコンテナを送信し、サービスプロバイダはセキュアコンテナを受信する
S14
サービスプロバイダは、ユーザにセキュアコンテナを送信し、ユーザはセキュアコンテナを受信する
S15
ユーザは、課金処理を実行する
S16
ユーザは、コンテンツを再生する
S17
エンド
B

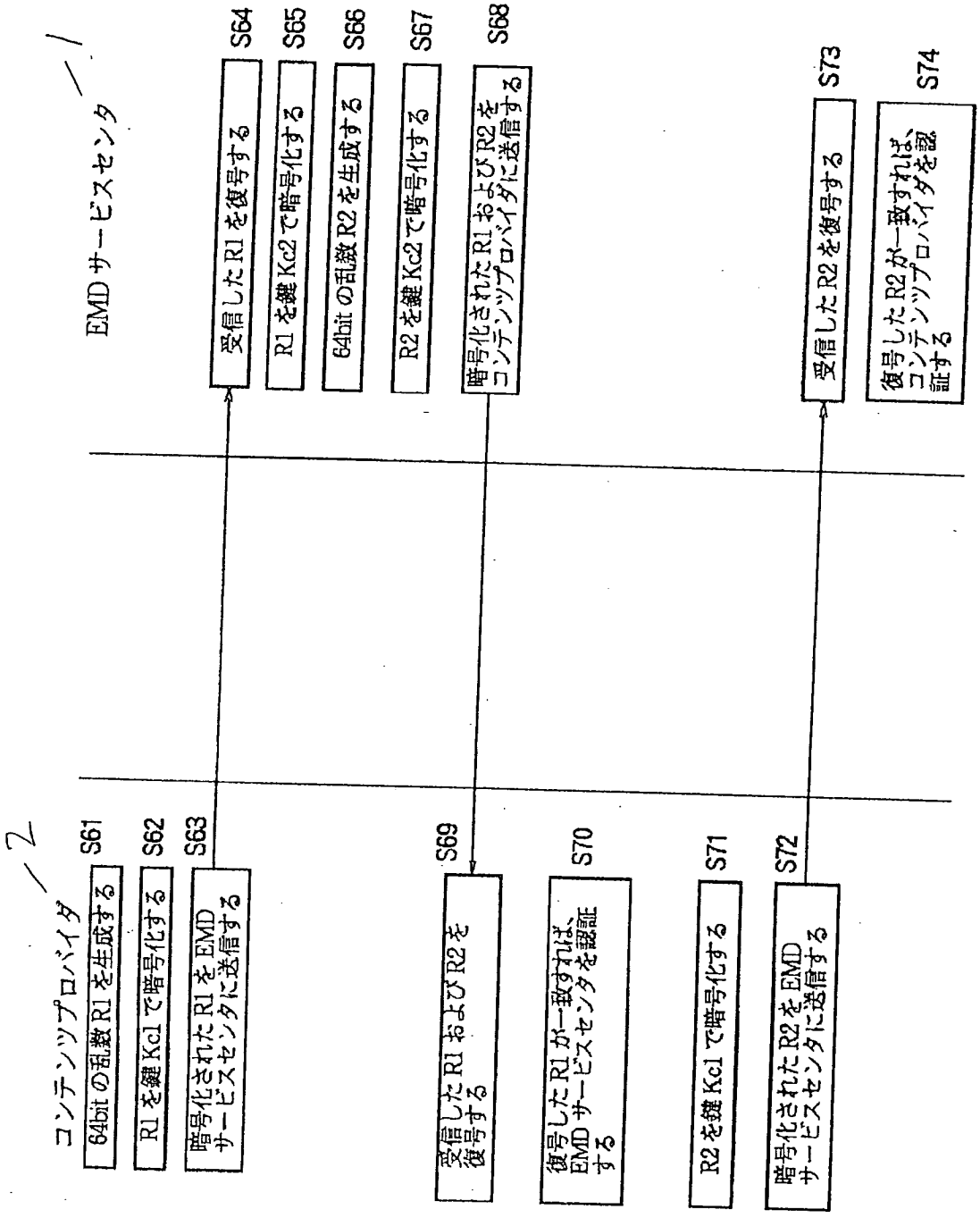
【図３５】


コンテンツ配布処理スタート
A
EMDサービスセンタは，コンテンツプロバイダに配送用鍵を送信し、コンテンツプロバイダは配送鍵を受信する
S21
EMDサービスセンタは，サービスプロバイダに配送用鍵を送信し、サービスプロバイダは配送鍵を受信する
S22
ユーザは，機器情報をEMDサービスセンタに登録する
S23
EMDサービスセンタは、ユーザに配送用鍵を送信し、ユーザは配送用鍵を受信する
S24
コンテンツプロバイダは、サービスプロバイダにセキュアコンテナを送信し、サービスプロバイダはセキュアコンテナを受信する
S25
サービスプロバイダは、ユーザにセキュアコンテナを送信し、ユーザはセキュアコンテナを受信する
S26
ユーザは、課金処理を実行する
S27
ユーザは、コンテンツを再生する
S28
エンド
B

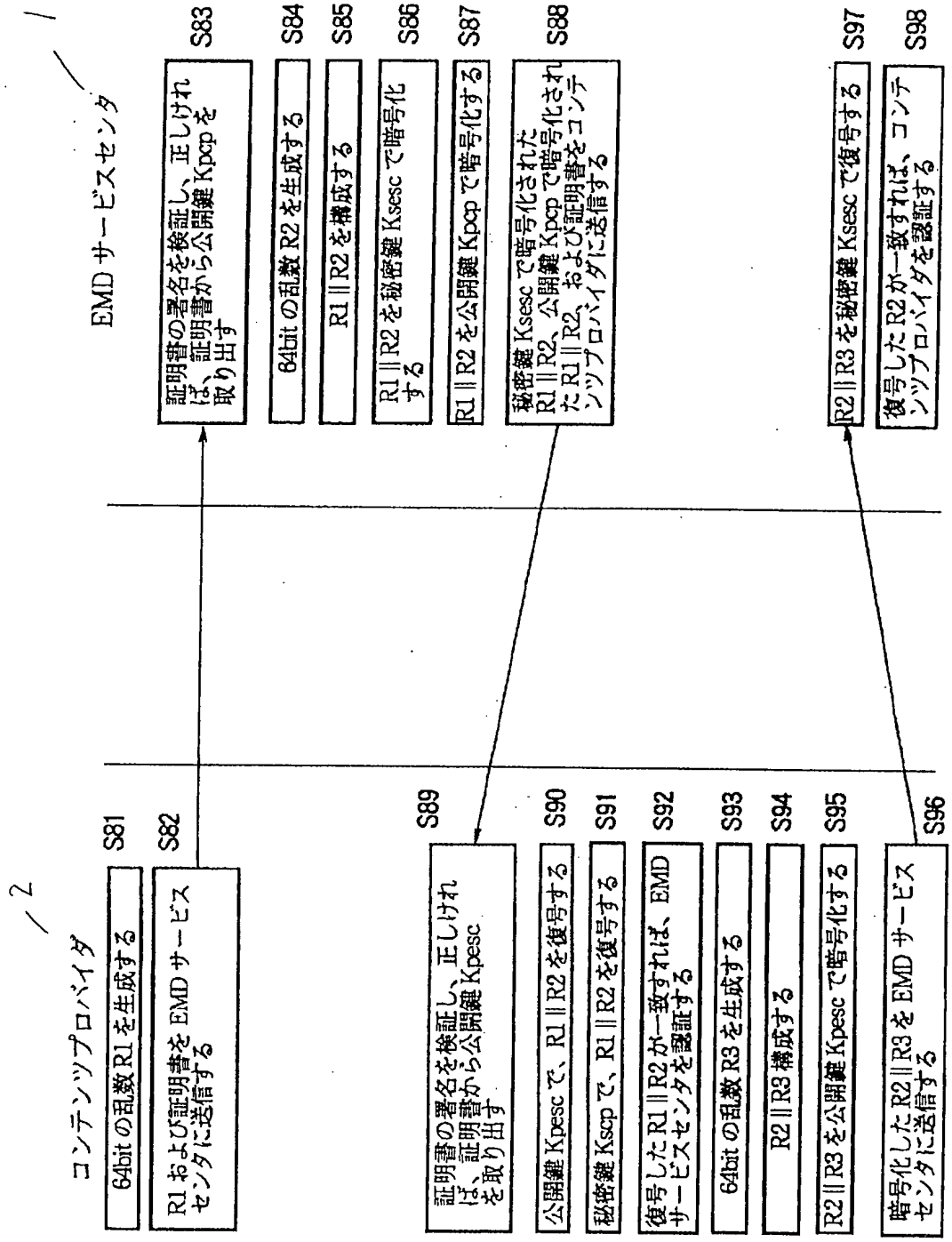
【図３７】


EMD サービスセンタ
1
コンテンツプロバイダ
2
S41
64bit の乱数 R1 を生成する
S42
R1 を鍵 Kc で暗号化する
S43
暗号化された R1 を EMD サービスセンタに送信する
S44
受信した R1 を復号する
S45
32bit の乱数 R2 を生成する
S46
乱数 R1 の下位 32bit を乱数 R2 で入れ替え、R1H‖R2 を得る
S47
R1H‖R2 を鍵 Kc で暗号化する
S48
暗号化された R1H‖R2 をコンテンツプロバイダに送信する
S49
受信した R1H‖R2 を復号する
S50
復号した R1H‖R2 の上位 32 bit が一致すれば、EMD サービスセンタを認証する
S51
32bit の乱数 R3 を生成する
S52
R2‖R3 を構成する
S53
R2‖R3 を鍵 Kc で暗号化する
S54
暗号化された R2‖R3 を EMD サービスセンタに送信する
S55
受信した R2‖R3 を復号する
S56
復号した R2‖R3 の上位 32 bit が一致すれば、コンテンツプロバイダを認証する

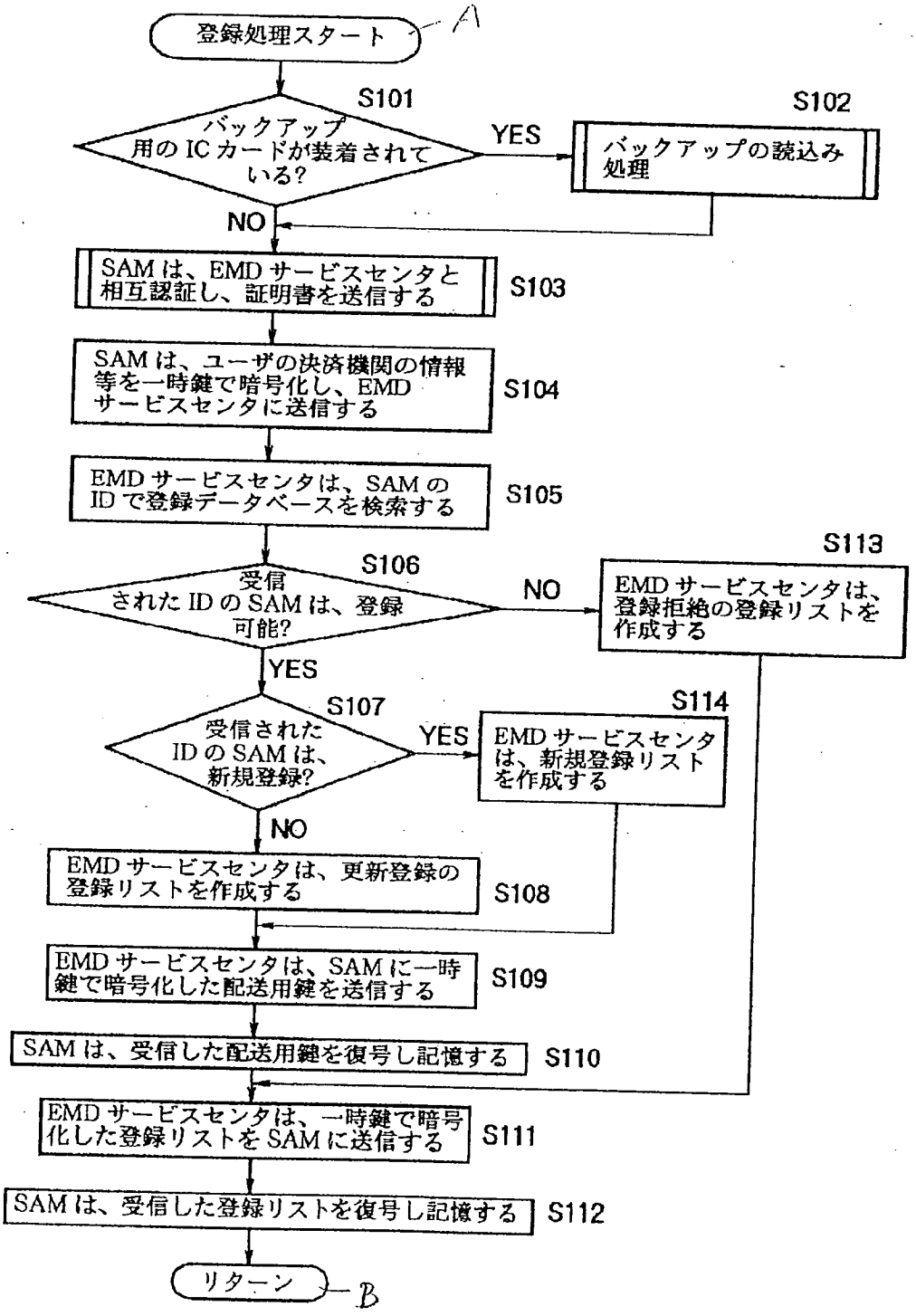
【図３８】


EMDサービスセンタ
1
コンテンツプロバイダ
2
S61
64bitの乱数R1を生成する
S62
R1を鍵Kc1で暗号化する
S63
暗号化されたR1をEMDサービスセンタに送信する
S64
受信したR1を復号する
S65
R1を鍵Kc2で暗号化する
S66
64bitの乱数R2を生成する
S67
R2を鍵Kc2で暗号化する
S68
暗号化されたR1およびR2をコンテンツプロバイダに送信する
S69
受信したR1およびR2を復号する
S70
復号したR1が一致すれば、EMDサービスセンタを認証する
S71
R2を鍵Kc1で暗号化する
S72
暗号化されたR2をEMDサービスセンタに送信する
S73
受信したR2を復号する
S74
復号したR2が一致すれば、コンテンツプロバイダを認証する

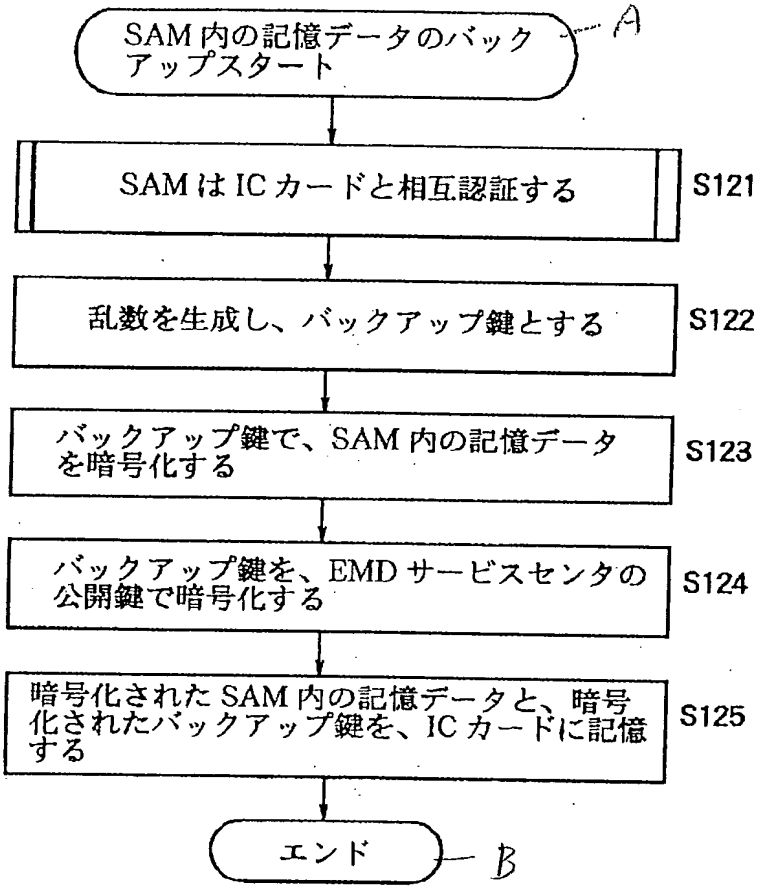
【図３９】


1
EMD サービスセンタ
2
コンテンツプロバイダ
S81
64bit の乱数 R1 を生成する
S82
R1 および証明書を EMD サービスセンタに送信する
S83
証明書の署名を検証し、正しければ、証明書から公開鍵 Kpcp を取り出す
S84
64bit の乱数 R2 を生成する
S85
R1 || R2 を構成する
S86
R1 || R2 を秘密鍵 Ksesc で暗号化する
S87
R1 || R2 を公開鍵 Kpcp で暗号化する
S88
秘密鍵 Ksesc で暗号化された R1 || R2、公開鍵 Kpcp で暗号化されたコンテンツプロバイダおよび証明書をコンテンツプロバイダに送信する
S89
証明書の署名を検証し、正しければ、証明書から公開鍵 Kpesc を取り出す
S90
公開鍵 Kpesc で、R1 || R2 を復号する
S91
秘密鍵 Kscp で、R1 || R2 を復号する
S92
復号した R1 || R2 が一致すれば、EMD サービスセンタを認証する
S93
64bit の乱数 R3 を生成する
S94
R2 || R3 構成する
S95
R2 || R3 を公開鍵 Kpesc で暗号化する
S96
暗号化した R2 || R3 を EMD サービスセンタに送信する
S97
R2 || R3 を秘密鍵 Ksesc で復号する
S98
復号した R2 が一致すれば、コンテンツプロバイダを認証する

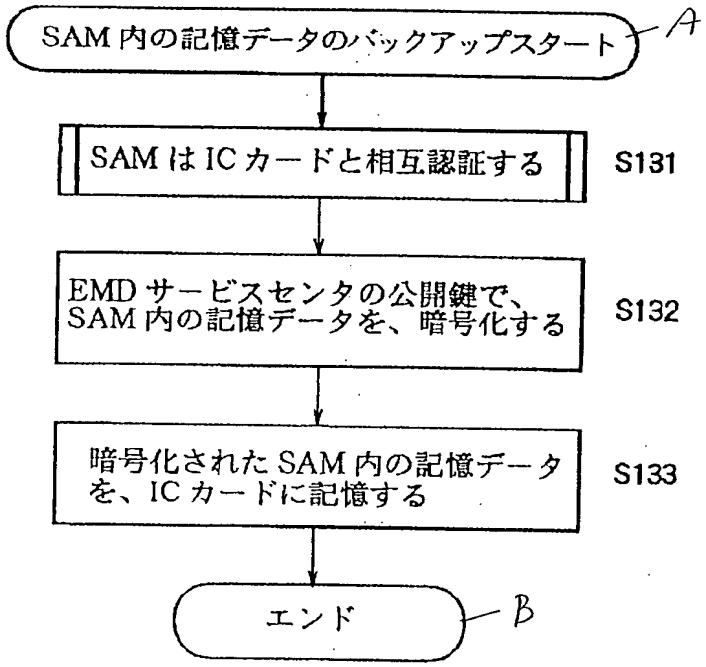
【図４０】


登録処理スタート
A
S101
バックアップ用のICカードが装着されている?
YES
S102
バックアップの読込み処理
NO
SAMは、EMDサービスセンタと相互認証し、証明書を送信する
S103
SAMは、ユーザの決済機関の情報等を一時鍵で暗号化し、EMDサービスセンタに送信する
S104
EMDサービスセンタは、SAMのIDで登録データベースを検索する
S105
S106
受信されたIDのSAMは、登録可能?
NO
S113
EMDサービスセンタは、登録拒絶の登録リストを作成する
YES
S107
受信されたIDのSAMは、新規登録?
YES
S114
EMDサービスセンタは、新規登録リストを作成する
NO
EMDサービスセンタは、更新登録の登録リストを作成する
S108
EMDサービスセンタは、SAMに一時鍵で暗号化した配送用鍵を送信する
S109
SAMは、受信した配送用鍵を復号し記憶する
S110
EMDサービスセンタは、一時鍵で暗号化した登録リストをSAMに送信する
S111
SAMは、受信した登録リストを復号し記憶する
S112
リターン
B

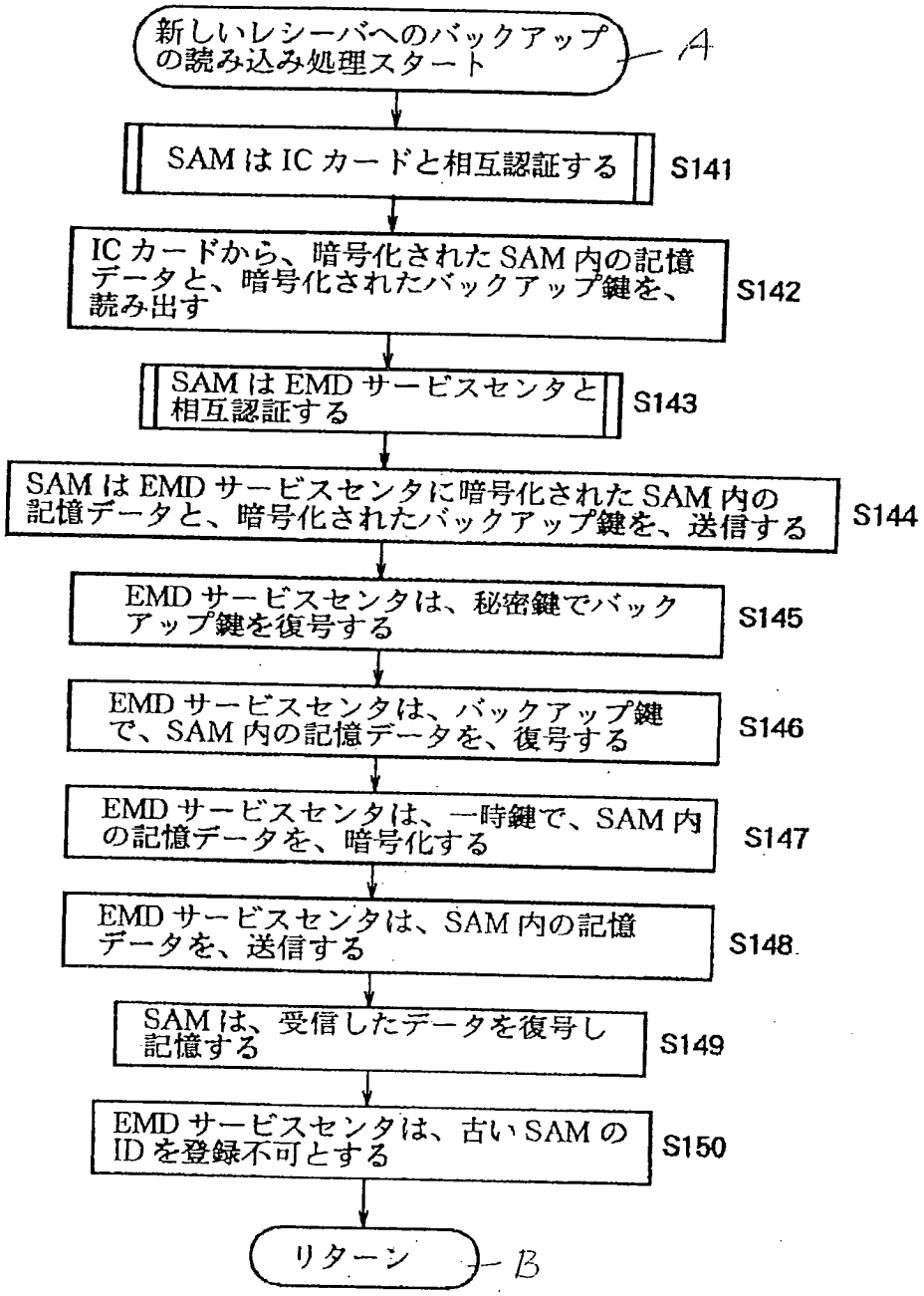
【図４３】


SAM内の記憶データのバックアップスタート
A
SAMはICカードと相互認証する
S121
乱数を生成し、バックアップ鍵とする
S122
バックアップ鍵で、SAM内の記憶データを暗号化する
S123
バックアップ鍵を、EMDサービスセンタの公開鍵で暗号化する
S124
暗号化されたSAM内の記憶データと、暗号化されたバックアップ鍵を、ICカードに記憶する
S125
エンド
B

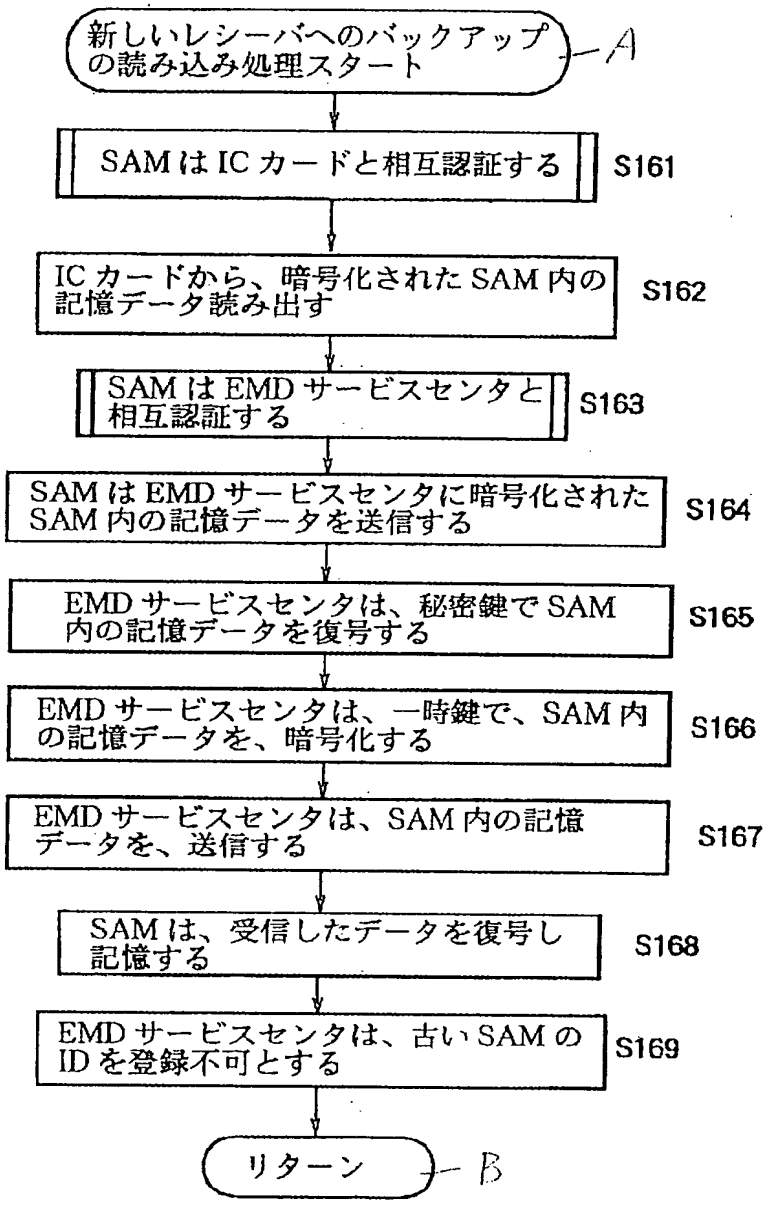
【図４４】


SAM内の記憶データのバックアップスタート
A
SAMはICカードと相互認証する
S131
EMDサービスセンタの公開鍵で、SAM内の記憶データを、暗号化する
S132
暗号化されたSAM内の記憶データを、ICカードに記憶する
S133
エンド
B

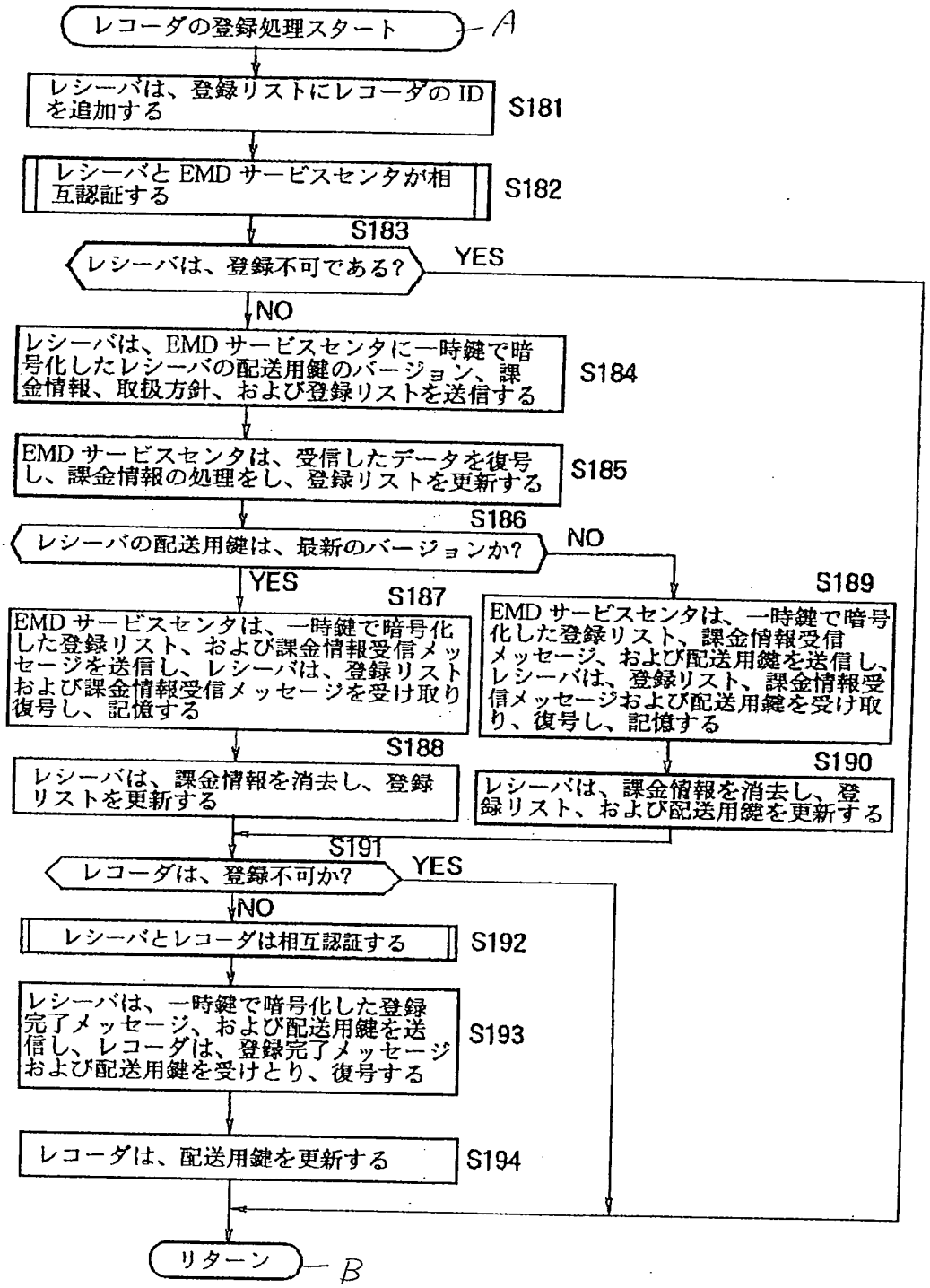
【図４５】


新しいレシーバへのバックアップの読み込み処理スタート
A
SAMはICカードと相互認証する
S141
ICカードから、暗号化されたSAM内の記憶データと、暗号化されたバックアップ鍵を、読み出す
S142
SAMはEMDサービスセンタと相互認証する
S143
SAMはEMDサービスセンタに暗号化されたSAM内の記憶データと、暗号化されたバックアップ鍵を、送信する
S144
EMDサービスセンタは、秘密鍵でバックアップ鍵を復号する
S145
EMDサービスセンタは、バックアップ鍵で、SAM内の記憶データを、復号する
S146
EMDサービスセンタは、一時鍵で、SAM内の記憶データを、暗号化する
S147
EMDサービスセンタは、SAM内の記憶データを、送信する
S148
SAMは、受信したデータを復号し記憶する
S149
EMDサービスセンタは、古いSAMのIDを登録不可とする
S150
リターン
B

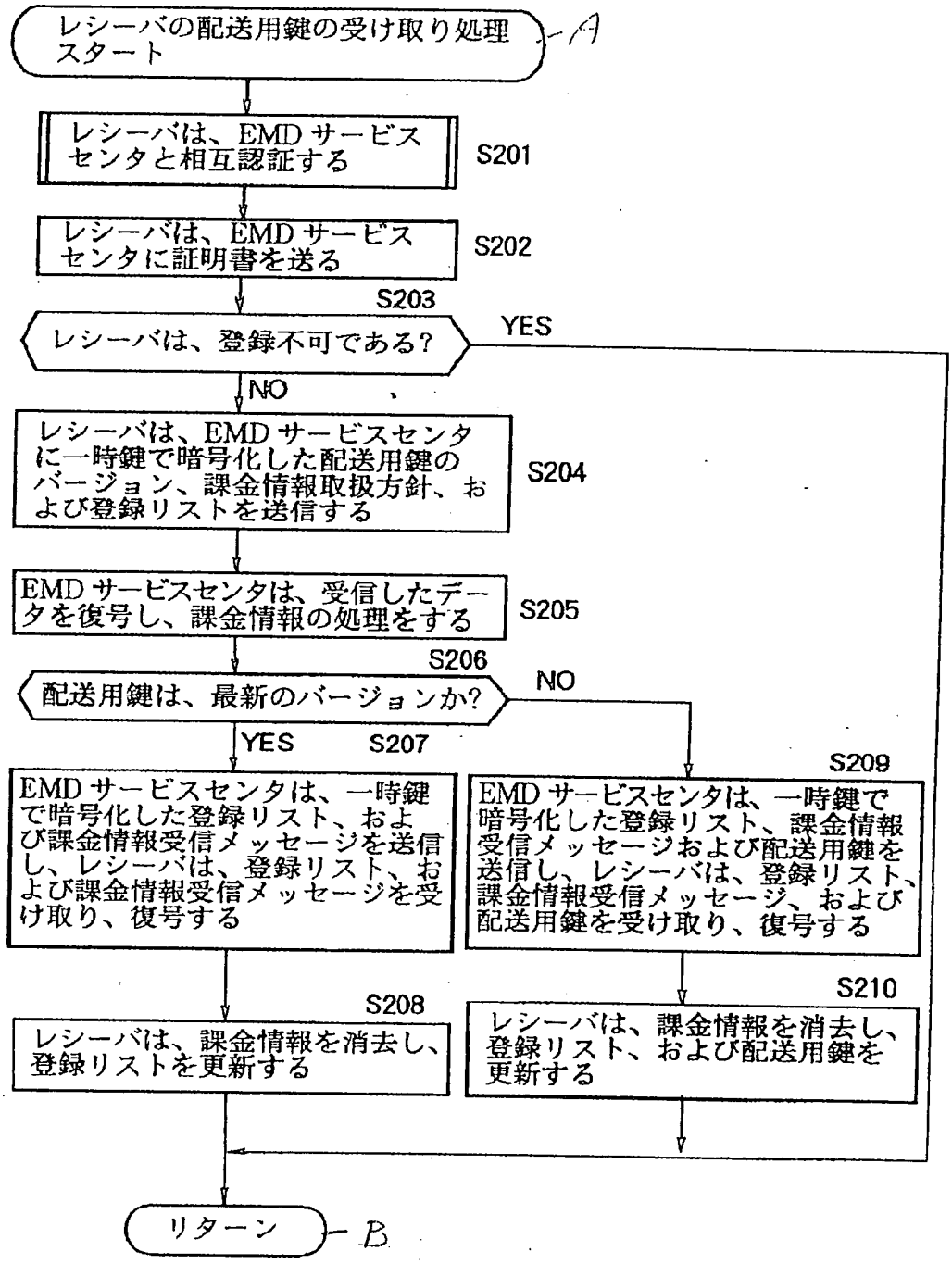
【図４６】


新しいレシーバへのバックアップの読み込み処理スタート
A
SAMはICカードと相互認証する
S161
ICカードから、暗号化されたSAM内の記憶データ読み出す
S162
SAMはEMDサービスセンタと相互認証する
S163
SAMはEMDサービスセンタに暗号化されたSAM内の記憶データを送信する
S164
EMDサービスセンタは、秘密鍵でSAM内の記憶データを復号する
S165
EMDサービスセンタは、一時鍵で、SAM内の記憶データを、暗号化する
S166
EMDサービスセンタは、SAM内の記憶データを、送信する
S167
SAMは、受信したデータを復号し記憶する
S168
EMDサービスセンタは、古いSAMのIDを登録不可とする
S169
リターン
B

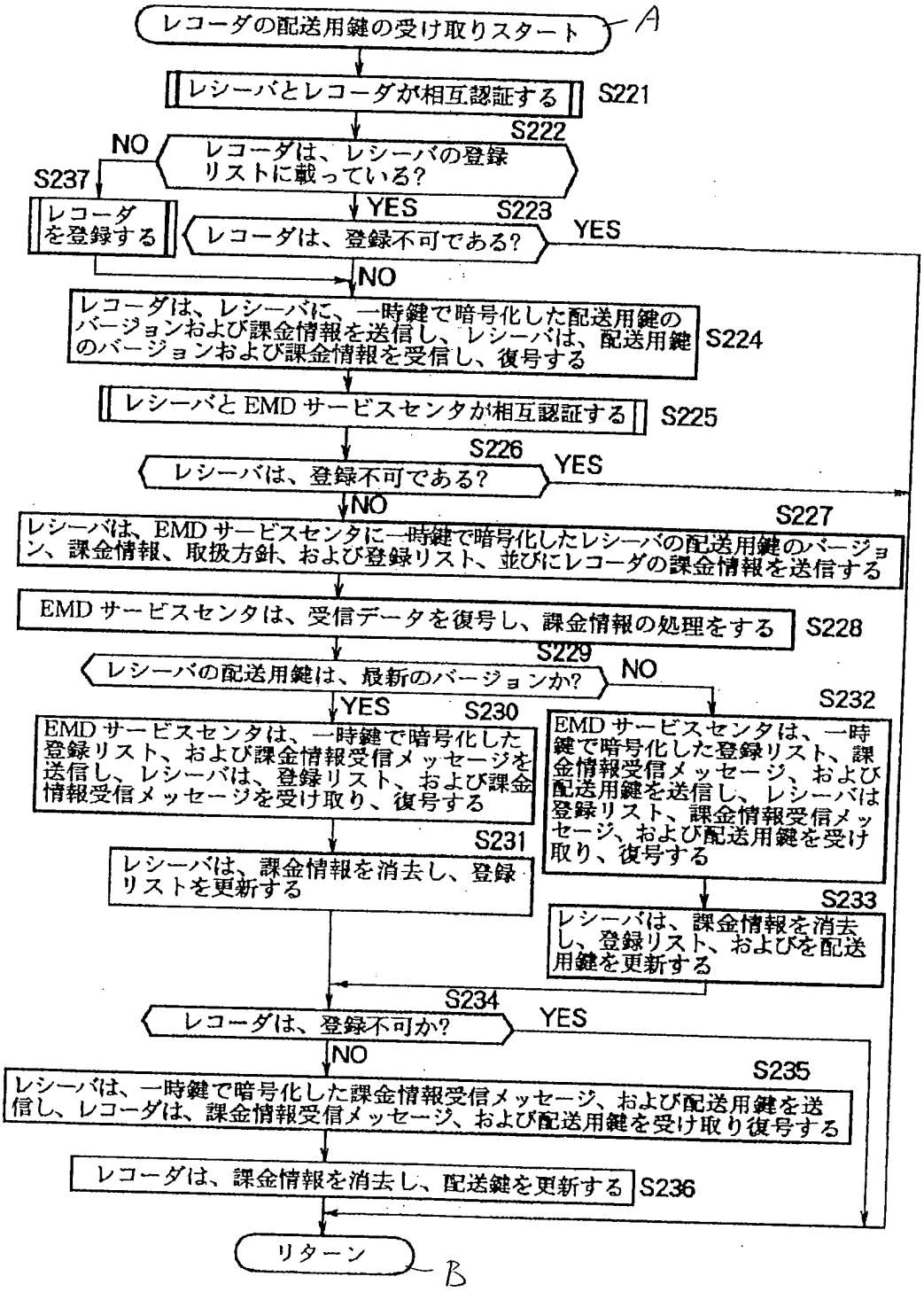
【図４７】


レコーダの登録処理スタート
A
レシーバは、登録リストにレコーダのIDを追加する
S181
レシーバとEMDサービスセンタが相互認証する
S182
S183
レシーバは、登録不可である?
YES
NO
レシーバは、EMDサービスセンタに一時鍵で暗号化したレシーバの配送用鍵のバージョン、課金情報、取扱方針、および登録リストを送信する
S184
EMDサービスセンタは、受信したデータを復号し、課金情報の処理をし、登録リストを更新する
S185
S186
レシーバの配送用鍵は、最新のバージョンか?
NO
YES
S187
EMDサービスセンタは、一時鍵で暗号化した登録リスト、および課金情報受信メッセージを送信し、レシーバは、登録リストおよび課金情報受信メッセージを受け取り復号し、記憶する
S189
EMDサービスセンタは、一時鍵で暗号化した登録リスト、課金情報受信メッセージ、および配送用鍵を送信し、レシーバは、登録リスト、課金情報受信メッセージおよび配送用鍵を受け取り、復号し、記憶する
S188
レシーバは、課金情報を消去し、登録リストを更新する
S190
レシーバは、課金情報を消去し、登録リスト、および配送用鍵を更新する
S191
レコーダは、登録不可か?
YES
NO
レシーバとレコーダは相互認証する
S192
レシーバは、一時鍵で暗号化した登録完了メッセージ、および配送用鍵を送信し、レコーダは、登録完了メッセージおよび配送用鍵を受けとり、復号する
S193
レコーダは、配送用鍵を更新する
S194
リターン
B

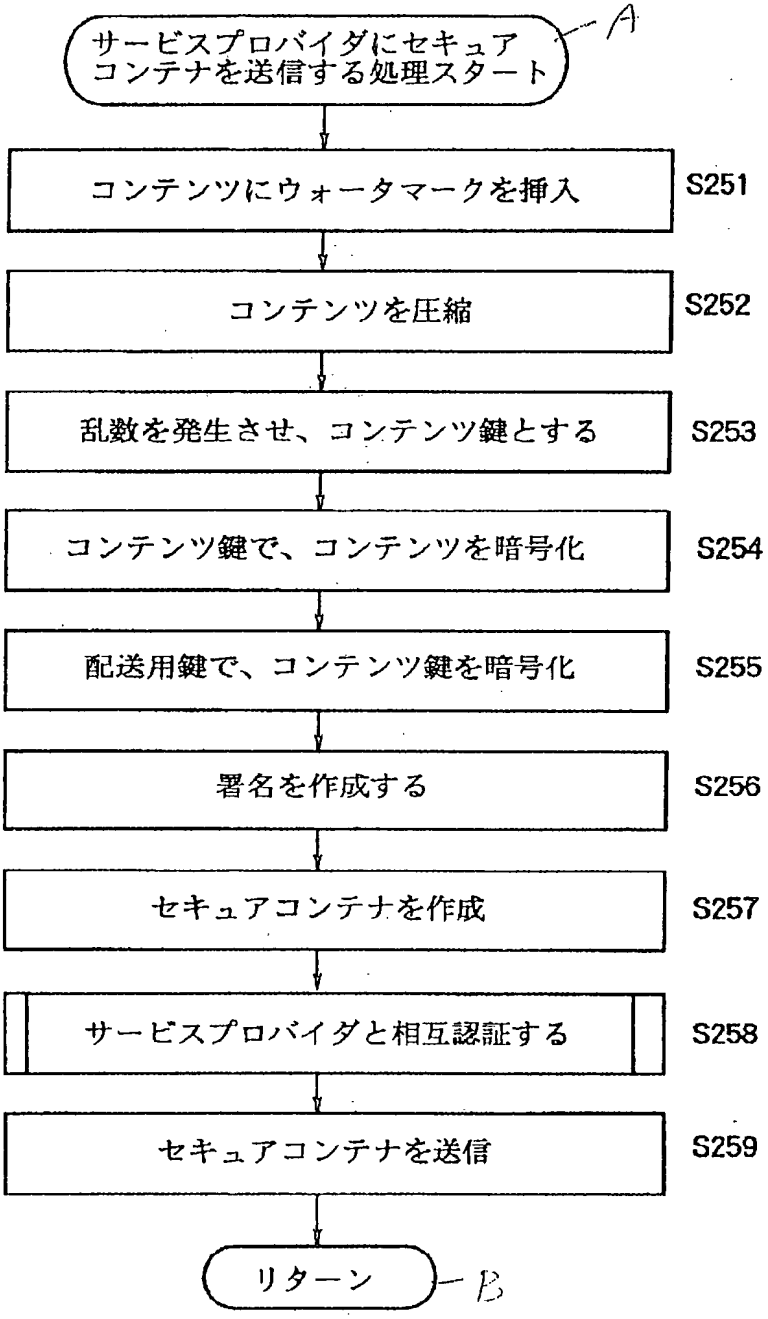
【図４８】


レシーバの配送用鍵の受け取り処理スタート
A
レシーバは、EMD サービスセンタと相互認証する
S201
レシーバは、EMD サービスセンタに証明書を送る
S202
S203
レシーバは、登録不可である?
YES
NO
レシーバは、EMD サービスセンタに一時鍵で暗号化した配送用鍵のバージョン、課金情報取扱方針、および登録リストを送信する
S204
EMD サービスセンタは、受信したデータを復号し、課金情報の処理をする
S205
S206
配送用鍵は、最新のバージョンか?
NO
YES
S207
EMD サービスセンタは、一時鍵で暗号化した登録リスト、および課金情報受信メッセージを送信し、レシーバは、登録リスト、および課金情報受信メッセージを受け取り、復号する
S209
EMD サービスセンタは、一時鍵で暗号化した登録リスト、課金情報受信メッセージおよび配送用鍵を送信し、レシーバは、登録リスト、課金情報受信メッセージ、および配送用鍵を受け取り、復号する
S208
レシーバは、課金情報を消去し、登録リストを更新する
S210
レシーバは、課金情報を消去し、登録リスト、および配送用鍵を更新する
リターン
B

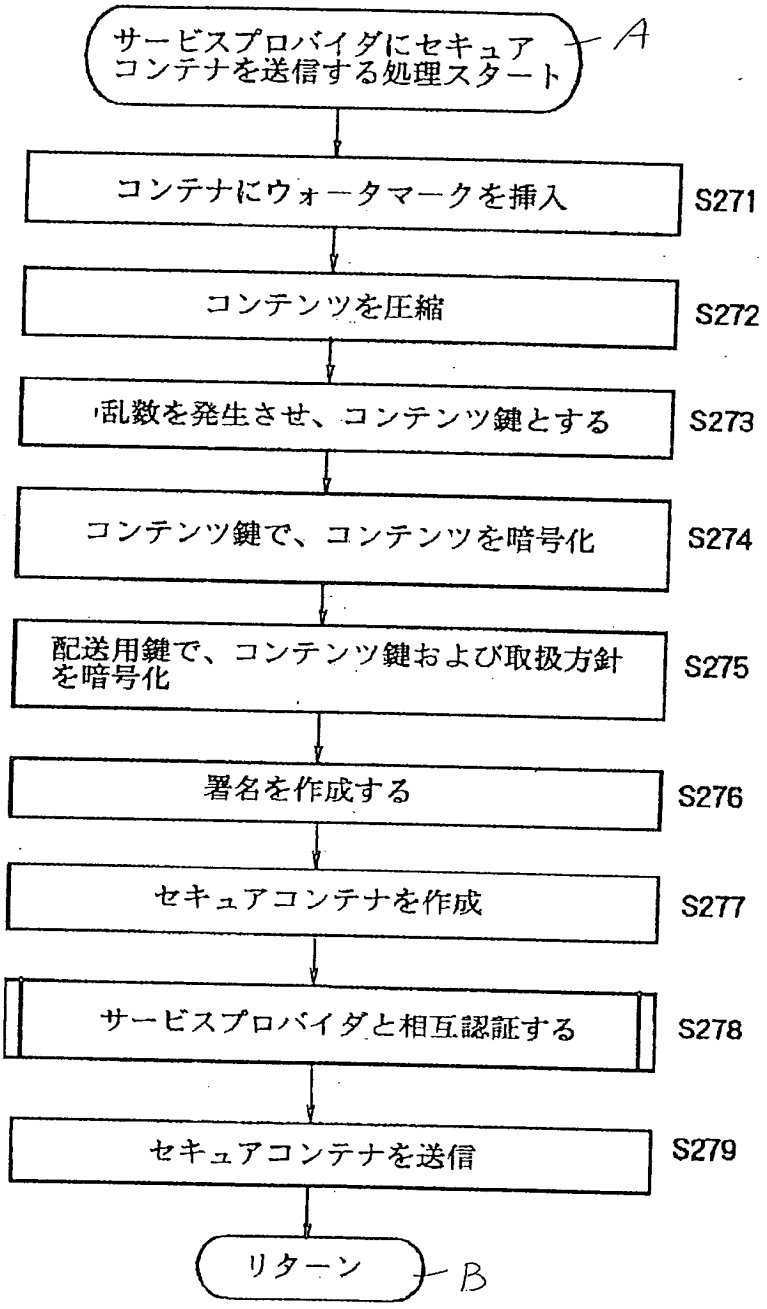
【図４９】


レコーダの配送用鍵の受け取りスタート
A
レシーバとレコーダが相互認証する
S221
S222
NO
レコーダは、レシーバの登録リストに載っている?
S237
レコーダを登録する
YES
S223
レコーダは、登録不可である?
YES
NO
レコーダは、レシーバに、一時鍵で暗号化した配送用鍵のバージョンおよび課金情報を送信し、レシーバは、配送用鍵のバージョンおよび課金情報を受信し、復号する
S224
レシーバとEMDサービスセンタが相互認証する
S225
S226
レシーバは、登録不可である?
YES
NO
S227
レシーバは、EMDサービスセンタに一時鍵で暗号化したレシーバの配送用鍵のバージョン、課金情報、取扱方針、および登録リスト、並びにレコーダの課金情報を送信する
EMDサービスセンタは、受信データを復号し、課金情報の処理をする
S228
S229
レシーバの配送用鍵は、最新のバージョンか?
NO
YES
S230
EMDサービスセンタは、一時鍵で暗号化した登録リスト、および課金情報受信メッセージを送信し、レシーバは、登録リスト、および課金情報受信メッセージを受け取り、復号する
S231
レシーバは、課金情報を消去し、登録リストを更新する
S232
EMDサービスセンタは、一時鍵で暗号化した登録リスト、課金情報受信メッセージ、および配送用鍵を送信し、レシーバは登録リスト、課金情報受信メッセージ、および配送用鍵を受け取り、復号する
S233
レシーバは、課金情報を消去し、登録リスト、およびを配送用鍵を更新する
S234
レコーダは、登録不可か?
YES
NO
S235
レシーバは、一時鍵で暗号化した課金情報受信メッセージ、および配送用鍵を送信し、レコーダは、課金情報受信メッセージ、および配送用鍵を受け取り復号する
レコーダは、課金情報を消去し、配送鍵を更新する
S236
リターン
B

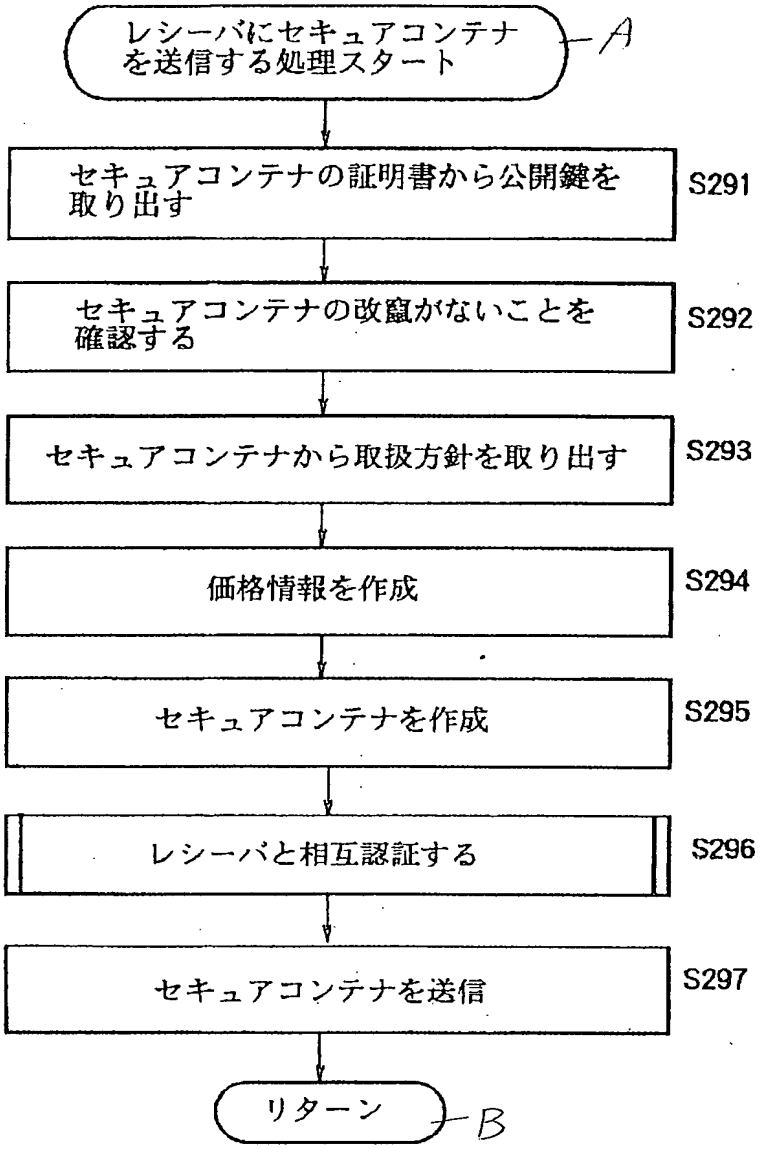
【図５０】


サービスプロバイダにセキュア
コンテナを送信する処理スタート
A
コンテンツにウォータマークを挿入
S251
コンテンツを圧縮
S252
乱数を発生させ、コンテンツ鍵とする
S253
コンテンツ鍵で、コンテンツを暗号化
S254
配送用鍵で、コンテンツ鍵を暗号化
S255
署名を作成する
S256
セキュアコンテナを作成
S257
サービスプロバイダと相互認証する
S258
セキュアコンテナを送信
S259
リターン
B

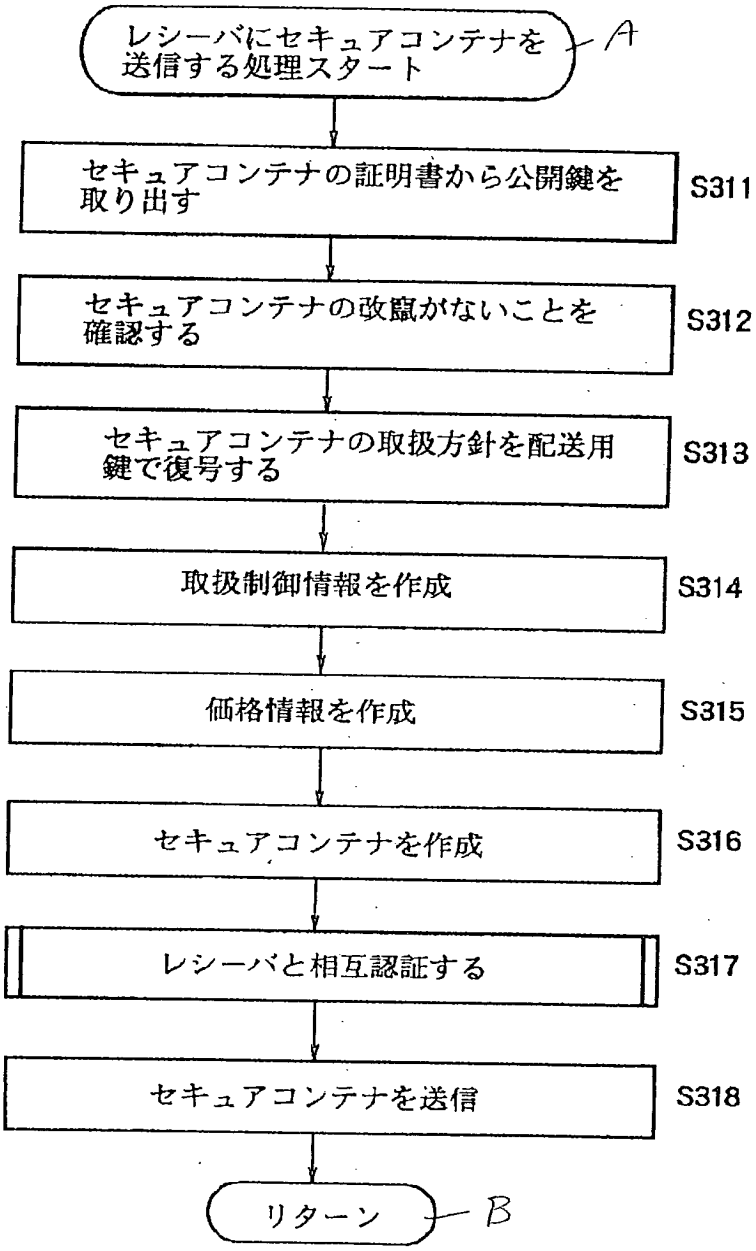
【図５１】


サービスプロバイダにセキュアコンテナを送信する処理スタート
A
コンテナにウォータマークを挿入
S271
コンテンツを圧縮
S272
乱数を発生させ、コンテンツ鍵とする
S273
コンテンツ鍵で、コンテンツを暗号化
S274
配送用鍵で、コンテンツ鍵および取扱方針を暗号化
S275
署名を作成する
S276
セキュアコンテナを作成
S277
サービスプロバイダと相互認証する
S278
セキュアコンテナを送信
S279
リターン
B

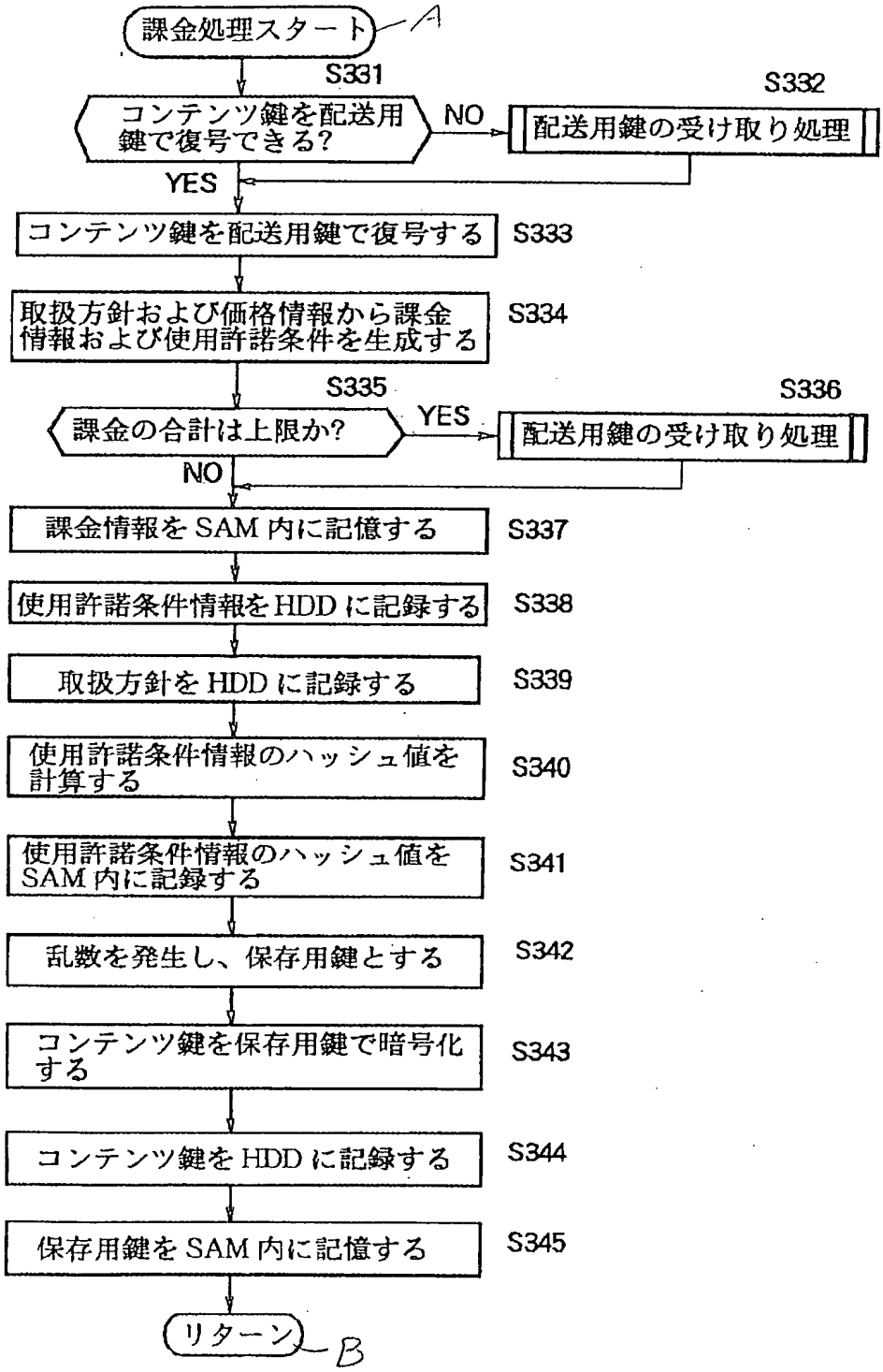
【図５２】


レシーバにセキュアコンテナを送信する処理スタート
A
セキュアコンテナの証明書から公開鍵を取り出す
S291
セキュアコンテナの改竄がないことを確認する
S292
セキュアコンテナから取扱方針を取り出す
S293
価格情報を作成
S294
セキュアコンテナを作成
S295
レシーバと相互認証する
S296
セキュアコンテナを送信
S297
リターン
B

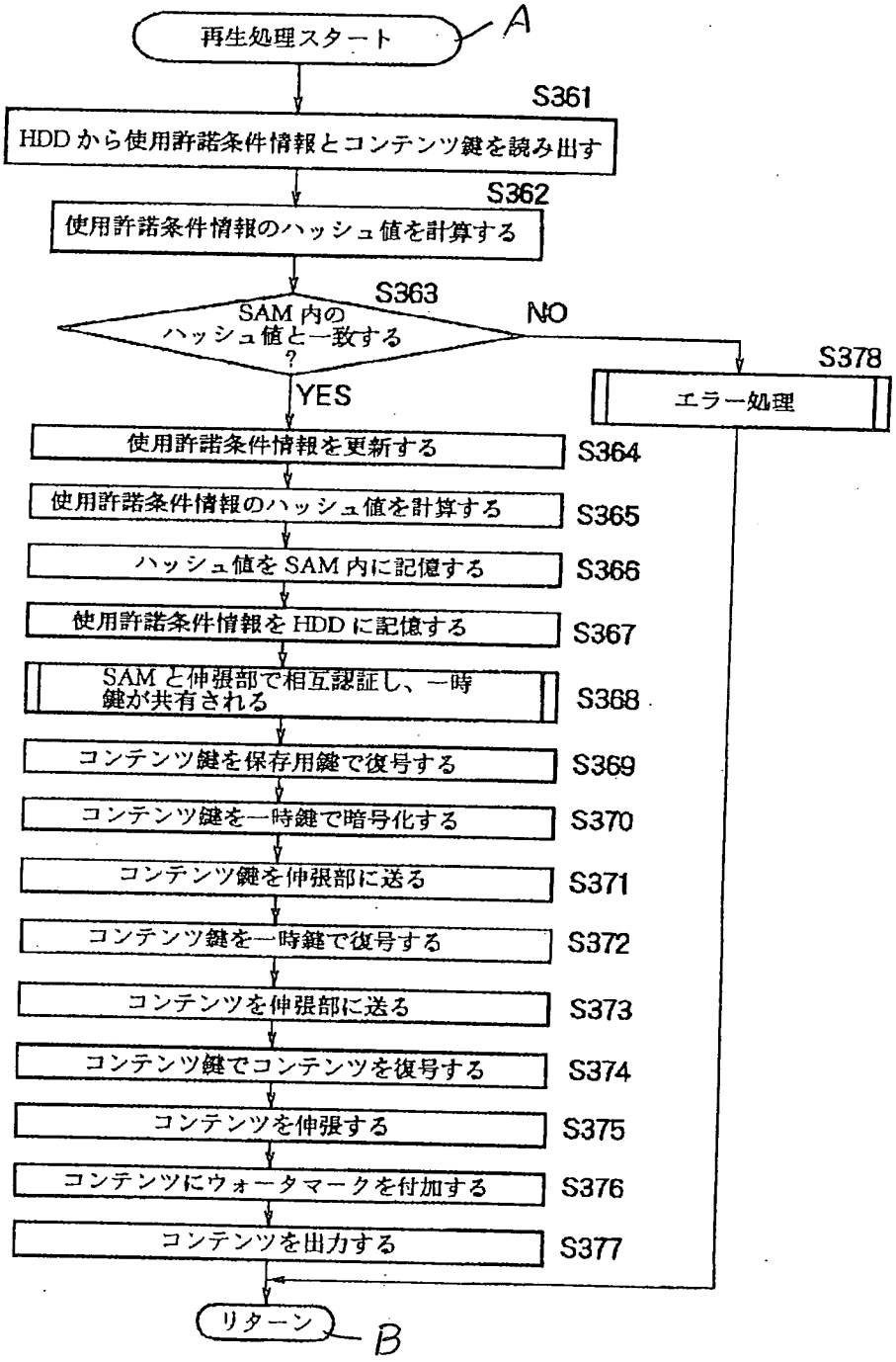
【図５３】


レシーバにセキュアコンテナを送信する処理スタート
A
セキュアコンテナの証明書から公開鍵を取り出す
S311
セキュアコンテナの改竄がないことを確認する
S312
セキュアコンテナの取扱方針を配送用鍵で復号する
S313
取扱制御情報を作成
S314
価格情報を作成
S315
セキュアコンテナを作成
S316
レシーバと相互認証する
S317
セキュアコンテナを送信
S318
リターン
B

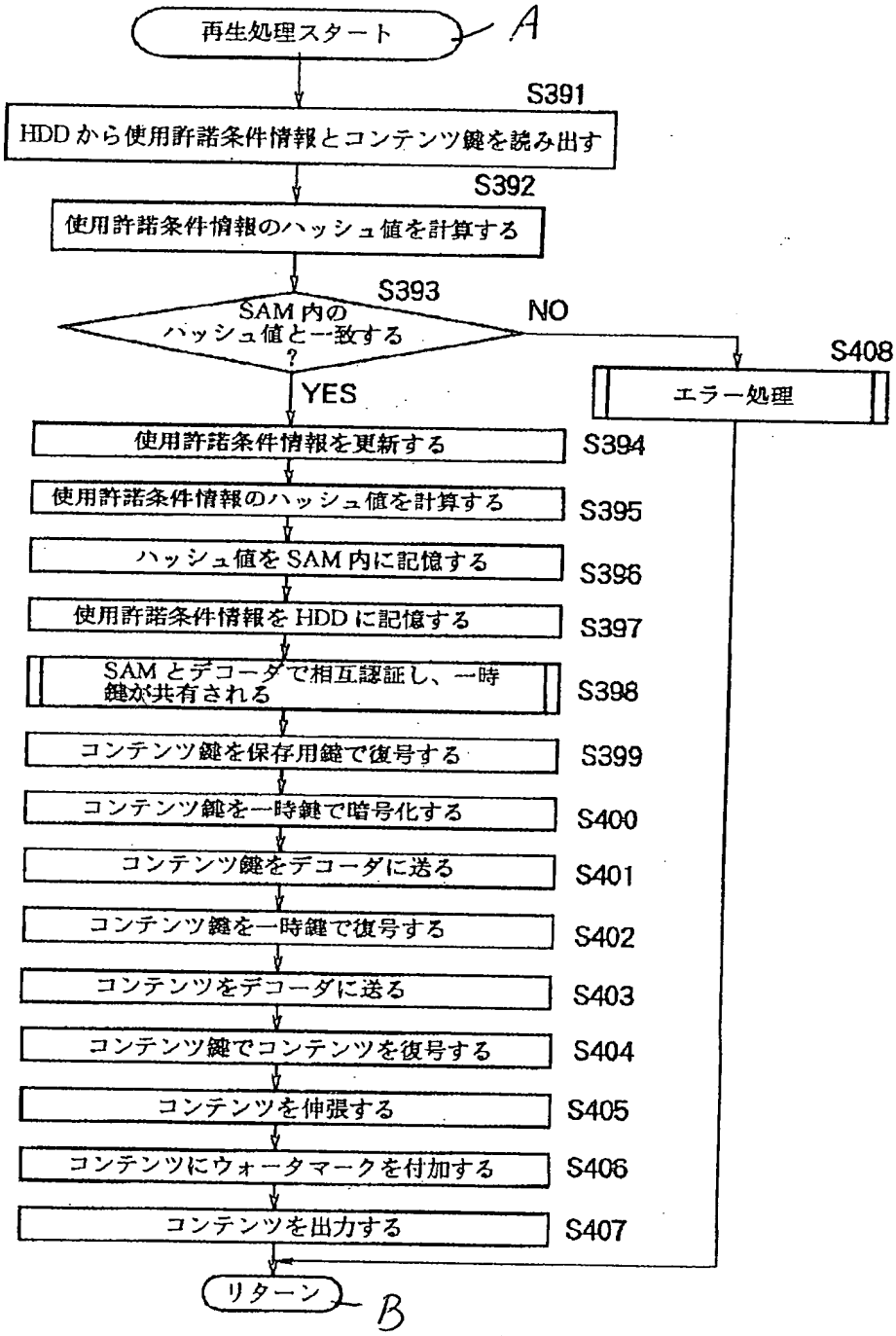
【図５４】


課金処理スタート
A
S331
コンテンツ鍵を配送用鍵で復号できる?
NO
S332
配送用鍵の受け取り処理
YES
コンテンツ鍵を配送用鍵で復号する
S333
取扱方針および価格情報から課金情報および使用許諾条件を生成する
S334
S335
課金の合計は上限か?
YES
S336
配送用鍵の受け取り処理
NO
課金情報をSAM内に記憶する
S337
使用許諾条件情報をHDDに記録する
S338
取扱方針をHDDに記録する
S339
使用許諾条件情報のハッシュ値を計算する
S340
使用許諾条件情報のハッシュ値をSAM内に記録する
S341
乱数を発生し、保存用鍵とする
S342
コンテンツ鍵を保存用鍵で暗号化する
S343
コンテンツ鍵をHDDに記録する
S344
保存用鍵をSAM内に記憶する
S345
リターン
B

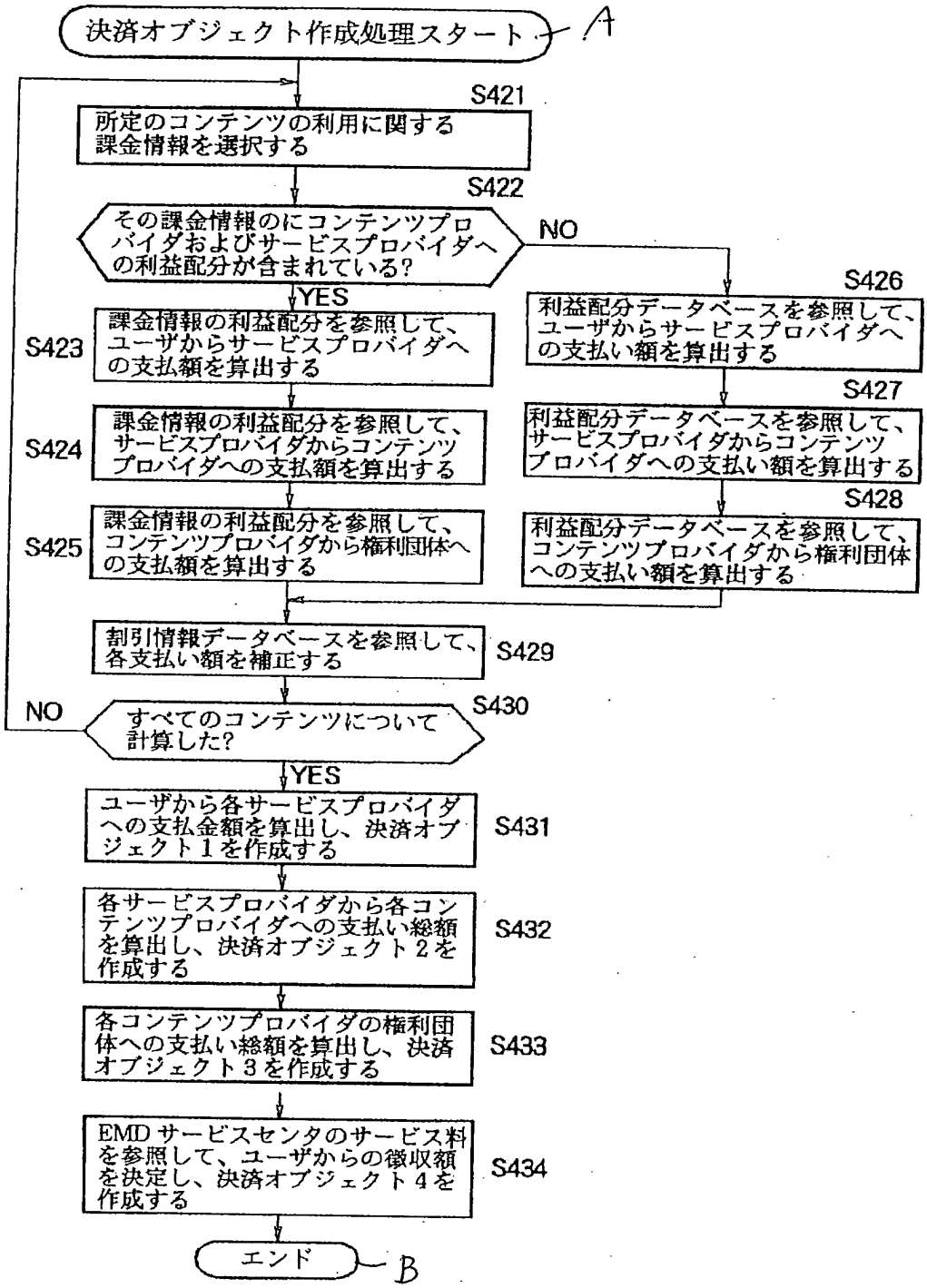
【図５５】


再生処理スタート
A
S361
HDDから使用許諾条件情報とコンテンツ鍵を読み出す
S362
使用許諾条件情報のハッシュ値を計算する
S363
SAM内のハッシュ値と一致する？
NO
S378
エラー処理
YES
使用許諾条件情報を更新する
S364
使用許諾条件情報のハッシュ値を計算する
S365
ハッシュ値をSAM内に記憶する
S366
使用許諾条件情報をHDDに記憶する
S367
SAMと伸張部で相互認証し、一時鍵が共有される
S368
コンテンツ鍵を保存用鍵で復号する
S369
コンテンツ鍵を一時鍵で暗号化する
S370
コンテンツ鍵を伸張部に送る
S371
コンテンツ鍵を一時鍵で復号する
S372
コンテンツを伸張部に送る
S373
コンテンツ鍵でコンテンツを復号する
S374
コンテンツを伸張する
S375
コンテンツにウォータマークを付加する
S376
コンテンツを出力する
S377
リターン
B

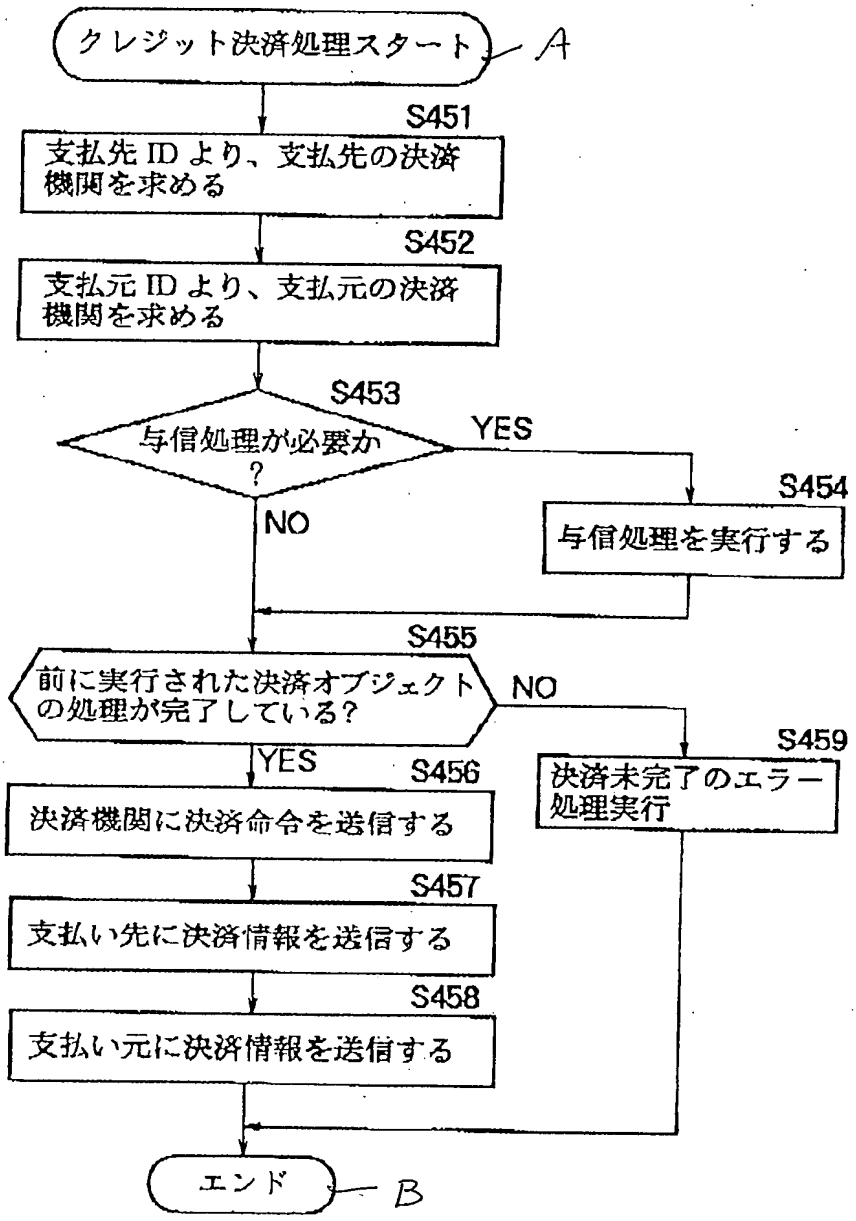
【図５６】


再生処理スタート
A
S391
HDDから使用許諾条件情報とコンテンツ鍵を読み出す
S392
使用許諾条件情報のハッシュ値を計算する
S393
SAM内のハッシュ値と一致する？
NO
S408
エラー処理
YES
使用許諾条件情報を更新する
S394
使用許諾条件情報のハッシュ値を計算する
S395
ハッシュ値をSAM内に記憶する
S396
使用許諾条件情報をHDDに記憶する
S397
SAMとデコーダで相互認証し、一時鍵が共有される
S398
コンテンツ鍵を保存用鍵で復号する
S399
コンテンツ鍵を一時鍵で暗号化する
S400
コンテンツ鍵をデコーダに送る
S401
コンテンツ鍵を一時鍵で復号する
S402
コンテンツをデコーダに送る
S403
コンテンツ鍵でコンテンツを復号する
S404
コンテンツを伸張する
S405
コンテンツにウォータマークを付加する
S406
コンテンツを出力する
S407
リターン
B

【図５７】


決済オブジェクト作成処理スタート
A
S421
所定のコンテンツの利用に関する課金情報を選択する
S422
その課金情報のにコンテンツプロバイダおよびサービスプロバイダへの利益配分が含まれている?
NO
YES
S426
利益配分データベースを参照して、ユーザからサービスプロバイダへの支払い額を算出する
S423
課金情報の利益配分を参照して、ユーザからサービスプロバイダへの支払額を算出する
S427
利益配分データベースを参照して、サービスプロバイダからコンテンツプロバイダへの支払い額を算出する
S424
課金情報の利益配分を参照して、サービスプロバイダからコンテンツプロバイダへの支払額を算出する
S428
利益配分データベースを参照して、コンテンツプロバイダから権利団体への支払い額を算出する
S425
課金情報の利益配分を参照して、コンテンツプロバイダから権利団体への支払額を算出する
S429
割引情報データベースを参照して、各支払い額を補正する
NO
S430
すべてのコンテンツについて計算した?
YES
S431
ユーザから各サービスプロバイダへの支払金額を算出し、決済オブジェクト１を作成する
S432
各サービスプロバイダから各コンテンツプロバイダへの支払い総額を算出し、決済オブジェクト２を作成する
S433
各コンテンツプロバイダの権利団体への支払い総額を算出し、決済オブジェクト３を作成する
S434
EMD サービスセンタのサービス料を参照して、ユーザからの徴収額を決定し、決済オブジェクト４を作成する
エンド
B

【図６１】


クレジット決済処理スタート
A
S451
支払先 ID より、支払先の決済機関を求める
S452
支払元 ID より、支払元の決済機関を求める
S453
与信処理が必要か？
YES
NO
S454
与信処理を実行する
S455
前に実行された決済オブジェクトの処理が完了している？
NO
YES
S456
決済機関に決済命令を送信する
S457
支払い先に決済情報を送信する
S458
支払い元に決済情報を送信する
S459
決済未完了のエラー処理実行
エンド
B